

Audit Report



YEAR 2000 ISSUES WITHIN U.S. EUROPEAN COMMAND
AND ITS SERVICE COMPONENTS

Report No. 99-145

April 30, 1999

Office of the Inspector General
Department of Defense

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

19990823 120

AB I99-11 2122

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

MARFOREUR	U.S. Marine Forces Europe
MTF	Medical Treatment Facility
NATO	North Atlantic Treaty Organization
NAVEUR	U.S. Naval Forces Europe
OASD(HA)	Office of the Assistant Secretary of Defense (Health Affairs)
RAF	Royal Air Force
SIPRNET	Secret Internet Protocol Router Network
USAFE	U.S. Air Forces in Europe
USAREUR	U.S. Army, Europe, and Seventh Army
USEUCOM	U.S. European Command
Y2K	Year 2000



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

April 30, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
COMMANDER IN CHIEF, U. S. EUROPEAN COMMAND
DIRECTOR, JOINT STAFF
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Year 2000 Issues Within U.S. European Command and Its
Service Components (Report No. 99-145)

We are providing this report for review and comment. This is a follow-on audit to the Army Audit Agency Memorandum Report No. AA 98-292, "U.S. European Command's Management of the Year 2000," July 30, 1998. We considered comments from the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the U.S. European Command, and the Army on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We request that the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional information on Recommendation 2.b. As a result of management comments, we added Recommendation 4. to the Joint Staff. Therefore, we request that the Joint Staff provide comments on Recommendation 4. We request that comments be provided by May 28, 1999.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172) (eklemstine@dodig.osd.mil) or Ms. Catherine M. Schneider at (703) 604-9609 (DSN 664-9609) (cschneider@dodig.osd.mil). See Appendix H for the report distribution. Audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-145
(Project No. 8LG-5039.01)

April 30, 1999

Year 2000 Issues Within U.S. European Command and Its Service Components

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 web page on the IGnet at <http://www.ignet.gov>.

Objectives. This is a follow-on audit to the Army Audit Agency Memorandum Report No. AA 98-292, "U.S. European Command's Management of the Year 2000," July 30, 1998. The overall audit objective was to evaluate the ability of the U.S. European Command to resolve year 2000 issues to avoid undue disruption of its mission.

Results. The U.S. European Command refined its overall year 2000 efforts and was making progress in addressing its year 2000 problems. Specifically, the U.S. European Command and its Service Components made significant progress in managing their year 2000 programs and were actively involved in resolving year 2000 issues. However, the U.S. European Command and its Service Components needed to take a number of additional measures to ensure successful year 2000 conversion. See the Finding section for details.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. European Command, through the U.S. European Command Year 2000 Task Force and in coordination with its Service Component year 2000 offices, ensure that users of the Carnegie Mellon database have the appropriate equipment that allows them to access the database; complete system architectures to determine year 2000 status for all mission-critical functional areas; assess the risk of establishing a moratorium on system changes during the last 3 months of calendar year 1999 versus fielding potentially unreliable systems; include a representative from the Command Surgeon's office on the U.S. European Command Year 2000 Task Force; coordinate with the Military Department medical commands, the Office of the Assistant Secretary of Defense (Health Affairs), and the U.S. Transportation Command to obtain the year 2000 status of health care systems used in the European theater; prepare all required operational contingency plans by March 31, 1999; include aircraft and weapon systems in the operational evaluation; issue guidance for uniformly addressing host nation infrastructure issues in the theater; establish a central office within the European theater for maintaining year 2000 compliance data on host nation infrastructure; and identify and validate year 2000 funding requirements. In addition, we recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issue and disseminate a users' manual for the Carnegie Mellon database and issue policy on the roles and responsibilities of the unified commands in addressing configuration management year 2000 issues. Also, we recommend that the Army Year 2000 Program Office issue operational contingency planning guidance. We recommend that the Joint

Staff modify operational evaluation guidance to clarify the scope of operational evaluations and initiate action to invite the North Atlantic Treaty Organization to participate in the U.S. European Command operational evaluation.

Management Comments. The U.S. European Command generally concurred with the recommendations, stating that it was distributing the Carnegie Mellon database to its Service Components via email; had completed the system architectures needed for the operational evaluation; would consider a moratorium on system changes based on a case-by-case risk assessment; had included a part-time representative from the Command Surgeon's office on the task force who had contacted various commands and the Joint Staff to obtain information on the status of health care systems used in the European theater; planned to have all operational contingency plans completed by September 30, 1999; planned to issue guidance on host nation support in August 1999; had designated the task force as the central office for maintaining year 2000 compliance data on host nation support; and had identified year 2000 funding requirements. The U.S. European Command partially concurred with the recommendations to include aircraft and weapon systems in the operational evaluation and to invite the North Atlantic Treaty Organization to participate in the operational evaluation, stating that its operational evaluation will only involve U.S. mission-critical joint systems, their interfaces with Service systems, and cross-Service systems and interfaces. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that users' manuals had been provided to the Joint Staff and that it was the Joint Staff's responsibility to provide them to the unified commands. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) also stated that the Office of the Secretary of Defense Year 2000 Program Office was working on configuration management policy. The Army concurred with the recommendation to issue operational contingency planning guidance. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. The U.S. European Command comments are generally responsive. Although the U.S. European Command did not have all its required operational contingency plans and continuity of operations plans prepared by March 31, 1999, as required by the "DoD Year 2000 Management Plan, Version 2.0" (DoD Management Plan), December 1998, its actions meet the intent of the recommendation. The U.S. European Command approach of completing and testing mission-critical plans by June 30, 1999, will meet the DoD Management Plan requirements. Although the U.S. European Command will not be able to complete the remaining plans until sometime after June 30, 1999, completion of those plans by September 30, 1999, should still provide the U.S. European Command with sufficient time to test the viability of those plans. The U.S. European Command comments on including aircraft and weapon systems in the operational evaluation are sufficiently responsive because they were complying with some of the Joint Staff criteria for conducting operational evaluations. The U.S. European Command comments on inviting the North Atlantic Treaty Organization to participate in the peacekeeping portion of the operational evaluation are generally responsive because the U.S. European Command cannot ensure that allied nation and coalition partner systems are operationally evaluated. As a result of those comments, we added recommendations to the Joint Staff. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments are generally responsive, but we are requesting additional information on the configuration management policy and an implementation date. We request that the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Joint Staff provide comments on the final report by May 28, 1999.

Table of Contents

Executive Summary	i
--------------------------	---

Introduction

Background	1
Objectives	2

Finding

Status of Year 2000 Issues Within U.S. European Command and the Service Components	3
--	---

Appendixes

A. Audit Process	
Scope	33
Methodology	34
B. Summary of Prior Coverage	36
C. Office of the Secretary of Defense Memorandums	37
D. Status of U.S. Army, Europe, and Seventh Army Year 2000 Program	39
E. Status of U.S. Naval Forces Europe Year 2000 Program	41
F. Status of U.S. Air Forces in Europe Year 2000 Program	47
G. Status of the North Atlantic Treaty Organization Year 2000 Program	50
H. Report Distribution	51

Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments	55
U.S. European Command Comments	56
Department of the Army Comments	63

Background

The year 2000 (Y2K) problem is the term most often used to describe the potential failure of information technology systems to process or perform date-related functions after 1999. The Y2K problem is rooted in the way that automated information systems record and compute dates. The U.S. military is highly dependent upon information technology – computer hardware and software. That information technology may not work if the programming cannot handle the Y2K date rollover. Because military operations depend on an infrastructure driven by information technology, commanders must ensure continuity of their mission capability despite Y2K risks of system or infrastructure degradation and failure.

Because of the potential failure of computers to run or function throughout the Government, the President issued an Executive Order, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the Y2K problem. The Executive Order also requires that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

DoD Y2K Management Plan. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is coordinating the overall DoD Y2K conversion effort. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued various iterations of the DoD Year 2000 Management Plan to provide direction and make the DoD Components responsible for implementing the five-phase Y2K management process. The "DoD Year 2000 Management Plan, Version 2.0" (DoD Management Plan), December 1998, is the most current iteration. The target completion date for implementation of mission-critical systems was December 31, 1998, and for non-mission-critical systems was March 31, 1999.

The Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff is the principal military adviser to the President, the Secretary of Defense, and the National Security Council. The Joint Chiefs of Staff have no executive authority to command the combatant forces. The Secretaries of the Military Departments assign all forces under their jurisdiction to the unified commands to perform missions assigned to those commands. The Joint Staff assists the Chairman of the Joint Chiefs of Staff with unified strategic direction of the combatant forces, unified operations of the combatant commands, and integration into an efficient team of air, land, and sea forces.

The "Joint Staff Year 2000 Action Plan" (the Action Plan), March 1998, provides the unified commands and Joint Staff directorates with the corporate strategy and management approach for addressing the Y2K problem. The Action Plan uses the same target completion date for the implementation phase as the DoD Management Plan. The Action Plan states that the goal is to have all warfighting (mission-critical) systems certified as Y2K compliant not later than December 31, 1998.

Office of the Secretary of Defense Memorandums. The Secretary of Defense and the Deputy Secretary of Defense have issued memorandums on DoD Y2K efforts. In the Secretary of Defense memorandum "Year 2000 Compliance," August 7, 1998, the Secretary of Defense stated that DoD was making insufficient progress on Y2K conversion, which he termed "a critical national defense issue." He directed a number of actions, including that the commander in chief of each unified command shall review the status of Y2K implementation within the command and subordinate units and formulate a Y2K operational evaluation plan. The Deputy Secretary of Defense issued a memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," August 24, 1998, which directed the Principal Staff Assistants of the Office of the Secretary of Defense to verify that all functions under their purview will continue unaffected by Y2K issues. Each Principal Staff Assistant was required to provide the Deputy Secretary of Defense with plans for Y2K-related end-to-end testing of each process within communications, health/medical, intelligence, logistics, and personnel. See Appendix C for more details on the Office of the Secretary of Defense memorandums.

U.S. European Command. The U.S. European Command (USEUCOM) is one of nine unified commands of DoD. On October 1, 1998, the USEUCOM area of responsibility expanded from 83 to 89 countries with the addition of 6 former states of the Soviet Union. A primary mission of USEUCOM is to provide combat forces to the North Atlantic Treaty Organization (NATO). In addition, USEUCOM conducts operations unilaterally or in concert with coalition partners. Service Components provide forces, as required, to support USEUCOM operations. The USEUCOM Service Components are the U.S. Army, Europe, and Seventh Army (USAREUR), U.S. Naval Forces Europe (NAVEUR), U.S. Air Forces in Europe (USAFE), U.S. Marine Forces Europe (MARFOREUR), and U.S. Special Operations Command Europe. In addition, Security Assistance Offices in several nations complement the U.S. military forces in the region by coordinating the efforts of USEUCOM with their respective host nations.

Objectives

This is a follow-on audit to the Army Audit Agency Memorandum Report No. AA 98-292, "U.S. European Command's Management of the Year 2000," July 30, 1998. The overall audit objective was to evaluate the ability of USEUCOM to resolve Y2K issues to avoid undue disruption of its mission. We did not review the management control program related to the overall audit objective because DoD recognizes the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance. See Appendix A for a discussion of the audit scope and methodology and Appendix B for a summary of prior coverage.

Status of Year 2000 Issues Within U.S. European Command and the Service Components

USEUCOM and its Service Components made significant progress in managing their Y2K programs and were actively involved in resolving Y2K issues. However, USEUCOM and its Service Components still need to:

- ensure that users of the DoD Y2K database are adequately trained and have appropriate equipment that allows them to access the database;
- complete system architectures to determine Y2K status of its systems;
- assess the risk of establishing a moratorium on system changes during the last 3 months of calendar year 1999 versus fielding potentially unreliable systems;
- uniformly develop operational contingency plans for missions that may be affected by the Y2K problem; and
- fully identify and validate Y2K funding requirements.

In addition, USEUCOM still needs to:

- include a representative from the Command Surgeon's office on the USEUCOM Y2K Task Force;
- coordinate with the Military Department medical commands, the Assistant Secretary of Defense (Health Affairs) (OASD[HA]), and the U.S. Transportation Command to obtain the Y2K status of health care systems used in the European theater;
- include aircraft and weapon systems in the USEUCOM draft operational evaluation plan;
- invite NATO to participate in the operational evaluation of peacekeeping operations;
- issue guidance for addressing host nation infrastructure issues; and
- establish a central point within the European theater for maintaining Y2K compliance data on host nation infrastructure.

Because of continuing operational commitments and international political instability in portions of its operating area, it is vital that USEUCOM have an aggressive and effective Y2K conversion program.

Army Audit Agency Report on USEUCOM Y2K Program

From February through March 1998, the Army Audit Agency conducted an audit to evaluate the status of the progress of USEUCOM in resolving its Y2K problems. Army Audit Agency Memorandum Report No. AA 98-292 made recommendations to USEUCOM and the Joint Staff. USEUCOM concurred with the recommendations and reported actions it was taking to implement those recommendations. In response to the recommendations from the Army Audit Agency, some of the actions USEUCOM took included:

- requiring USEUCOM headquarters directorates to submit quarterly reports on the Y2K status of their systems and
- requiring the Service Components to report monthly on the Y2K compliance of 10 functional areas: communications systems; infrastructure; intelligence, surveillance, and reconnaissance systems; mobility systems; non-nuclear command and control systems; nuclear command and control systems; personnel systems; sustainment systems; weapon systems; and any other issues that the Service Components chose to report on.

In addition, USEUCOM stated that it would perform operational impact assessments and prepare operational contingency plans once program managers delivered fixes or upgrades to their systems.

Theater Y2K Program Management

USEUCOM and its Service Components took numerous positive actions to address the Y2K problem and USEUCOM senior management reinforced the importance of the Y2K program throughout the command. To address the Y2K problem, each Service Component established an individual Y2K program based on guidance received from their Service headquarters. We visited USEUCOM headquarters and each Service Component and assessed the progress they had made in identifying and resolving Y2K problems. We issued memorandums to each Service Component on the status of their Y2K programs at the time of our visits. Our memorandums and the Service Components' responses are in Appendixes D, E, and F.

USEUCOM Y2K Program Management. USEUCOM took positive actions to address and resolve Y2K problems. The USEUCOM "Year 2000 Plan" (Y2K Plan), May 1, 1998, formalizes the command actions in the Y2K area. The Y2K Plan tasks USEUCOM headquarters to:

- identify and track all computer systems and embedded computer systems used at USEUCOM headquarters,
- involve operational users of systems in assessment of impacts of Y2K failures,
- formally request periodic detailed status of Y2K fixes from program managers of joint systems,
- require Y2K compliance language in all contracts, and
- actively request Service Component input on warfighting system Y2K issues.

In order to focus its Y2K efforts on operational readiness, USEUCOM transferred the responsibility for the Y2K program from the Command, Control, and Communications Systems Directorate to the Operations Directorate. In addition, in an October 21, 1998, message, USEUCOM established a task force to work full time on Y2K issues and to be the single point of contact for all Y2K functional issues and actions within the European theater. As of January 1999, the task force consisted of nine USEUCOM staff and three contractors. Additional contractors were to be hired to assist in planning for the operational evaluation scheduled in May 1999. Also in January 1999, the USEUCOM Task Force personnel visited each of the Service Components to assist them in resolving Y2K problems and to provide information on operational evaluation plans. Establishing the task force and visiting the Service Components assisted USEUCOM in its efforts to identify and prioritize mission-critical systems, help its Service Components identify their thin-line¹ of systems needed to perform mission-critical tasks, initiate the development of architectures for the USEUCOM operational evaluation, and plan for the operational evaluation. In addition, the task force met with functional counterparts at the Joint Staff and other unified commands to obtain information on resolving Y2K problems and planning for the operational evaluation.

USAREUR Y2K Program Management. USAREUR formally established a Y2K office within the Office of the Deputy Chief of Staff, Information Management. As of January 1999, the Y2K office had eight staff members. In addition, USAREUR established a tiger team with representation from each of its functional areas. The "USAREUR Year 2000 (Y2K) Management Plan," Revision II, January 7, 1999, outlines the overall strategy and guidance necessary to ensure that no mission-critical systems fail due to the Y2K problem. The Y2K management plan tasks USAREUR functional proponents and subordinate commands to:

- provide monthly reports to USAREUR on the status of their Y2K programs;

¹The minimum number of systems, interfaces, and applications needed to perform a task.

-
- provide quarterly briefings to either the USAREUR Deputy Commanding General or the Chief of Staff on the details of non-compliant systems; and
 - develop internal management plans that identify:
 - how they will address each of the five phases of the Y2K program,
 - the individual or position responsible for signing the certification documentation for mission-critical software,
 - the individual or position responsible for the non-information technology certification checklists, and
 - the reporting requirements for any lower level commands.

The USAREUR area support groups are responsible for facilities infrastructure. The USAREUR Y2K management plan tasks those groups to:

- identify, fund, and correct all Y2K vulnerabilities identified in on-post infrastructure;
- assess all items on their property books and hand receipts for Y2K impacts on military installations;
- be responsible for inventorying, assessing, testing, and certifying organic networks within their area support groups;
- develop contingency plans for all critical, non-compliant non-information technology systems; and
- brief the status of their Y2K program at quarterly base commanders' conferences.

As of January 22, 1999, the status of the Y2K program at USAREUR and its subordinate commands ranged from the end of the assessment phase at the area support groups to the start of the implementation phase (fix, repair, or ignore non-compliant systems/equipment) at 5th Signal Command.² Although the Office of the Deputy Chief of Staff, Information Management, manages the USAREUR Y2K program, functional staff at USAREUR subordinate commands are fully involved in the Y2K program. USAREUR staff correctly perceives the Y2K problem as an operational readiness issue rather than an information technology issue.

NAVEUR Y2K Program Management. NAVEUR established a Y2K program and took positive actions to address and resolve Y2K issues. The Command Y2K Project Office, Deputy Chief of Staff Command, Control, Communications, and Computers, was leading the NAVEUR Y2K effort. NAVEUR issued

²The 5th Signal Command is responsible for providing theater strategic, tactical, and installation signal support to U.S. and NATO warfighters in USEUCOM.

Commander, U.S. NAVEUR Instruction 2000.1, "COMUSNAVEUR Year 2000 (Y2K) Action Plan" (NAVEUR Y2K Action Plan), November 2, 1998. The NAVEUR Y2K Action Plan tasks subordinate commands to:

- identify and track all systems used within the NAVEUR area of responsibility,
- involve operational functional users of systems in assessment of the impact of Y2K failures,
- monitor the execution of Y2K corrections for systems within functional areas,
- write continuity of operations plans for all systems and facilities infrastructure determined to be mission-critical,
- successfully integrate all fielded systems and infrastructure, and
- prepare and submit monthly and quarterly reports.

As of October 1998, the NAVEUR functional staffs had not fully participated in the program. For example, the functional staffs were not involved in identifying mission-critical systems. In addition, NAVEUR had not determined critical missions or critical tasks that must be performed for critical missions. Also, NAVEUR was not proactively developing operational contingency plans. In an Inspector General, DoD, memorandum to NAVEUR, December 17, 1998, we raised those issues. NAVEUR responded with a memorandum, dated January 25, 1999, that described the actions taken since our visit. (See Appendix E for copies of the memorandums.) Specifically, NAVEUR:

- established an executive steering committee that meets weekly to monitor the implementation of the Instruction;
- assigned dedicated Y2K points of contact throughout the European theater;
- appointed Y2K functional points of contact to liaison with their counterparts on the USEUCOM Y2K Task Force;
- was in the process of categorizing non-compliant items as either mission-critical or mission support;
- was in the process of identifying systems requiring renovation that may impact operational readiness; and
- had developed 85 of 88 continuity of operations plans for mission-critical functions and expected to complete the 3 remaining plans by January 31, 1999.

In April 1999, we visited NAVEUR to perform followup work on the NAVEUR Y2K program. NAVEUR made substantial progress since our visit in October 1998, fully involving NAVEUR functional staffs in the Y2K program.

As of April 1999, the functional staffs had prioritized their mission-critical systems, had developed all of the needed continuity of operations plans, and perceived the Y2K problem as an operational readiness issue rather than an information technology issue.

USAFE Y2K Program Management. USAFE established a Y2K program and took positive actions to address and resolve Y2K issues. USAFE established a Y2K Program Management Office under the USAFE Computer Systems Squadron. In October 1998, the USAFE Y2K Program Management Office had six full-time and four part-time staff members. The USAFE "Year 2000 (Y2K) Guidance Package," September 15, 1997, provides USAFE and its wings/bases with an overall strategy on resolving the Y2K problem based on the DoD five-phase approach. Specifically, the USAFE plan tasks each wing/base to:

- establish Y2K project teams and working groups and develop organizational project management plans;
- inventory every system in the wing/base;
- prioritize systems for detailed analysis based on anticipated renovation approach and associated resources, availability and understandability of system documentation, interface dependencies, life expectancy, mission criticality, subsystem dependencies, system age, and system size;
- confirm schedules for the retirement, replacement, or redevelopment of systems;
- conduct a detailed analysis on every system to determine the extent to which the systems are affected and develop contingency plans;
- identify alternatives for implementing systems;
- identify funding sources for implementation requirements; and
- develop emergency response strategy and determine use of emergency response teams.

Based on the requirements in the USAFE plan, USAFE established the Y2K Working Group and Base Y2K Working Groups to gather and disseminate information throughout the command.

Y2K Working Group. The USAFE Y2K Working Group consists of representatives from each functional area within USAFE headquarters. The group is responsible for coordinating with their respective functional area chain of command to ensure all Y2K issues are identified and resolved. Members of the USAFE Y2K Program Management Office serve as the chair and co-chair of the Y2K Working Group.

Base Y2K Working Groups. The Base Y2K Working Groups include representatives from all base activities. The groups are responsible for coordinating with their local activities to ensure all Y2K issues are identified and

resolved. The chair and co-chair of each group are from the Base Communications Squadron. The groups are responsible for reporting quarterly status to the USAFE Y2K Program Management Office and the local installation commander.

As of December 16, 1998, the status of the Y2K program at USAFE and its subordinate commands ranged from the end of the assessment phase at Aviano Air Base, Italy, to the start of the implementation phase at Royal Air Force (RAF) Lakenheath, United Kingdom. All functional areas of USAFE commands participated in the Y2K plan with assigned Y2K representatives at the squadron level. In an Inspector General, DoD, memorandum, January 12, 1999, we suggested that USAFE ensure that wing commanders be made aware of the Y2K status of all warfighting assets under their authority and that existing contingency plans be used to develop continuity of operations plans to ensure optimal use of resources. USAFE responded with a memorandum, dated February 25, 1999, that described the actions taken since our visit. (See Appendix F for copies of the memorandums.) Specifically, USAFE:

- expected to have all wing continuity of operations plans completed by March 15, 1999, and a comprehensive USAFE plan to be presented by April 15, 1999;
- contacted wing Y2K offices to ensure they had access to the Air Force Automated Systems Inventory database and supplemented database information with updates from the Air Force Materiel Command Y2K program office; and
- formed a Y2K tiger team, composed of experts from its directorates that have mission-critical Y2K vulnerabilities, to conduct staff visits to all six of the USAFE main operating bases in March and April 1999.

As of February 25, 1999, USAFE was in the process of developing overall wing and USAFE-wide continuity of operations plans, had disseminated Y2K compliance information on aircraft and weapon systems to wing and group³ commanders, and was placing more emphasis on areas where mission-critical Y2K vulnerabilities existed.

MARFOREUR Y2K Program Management. MARFOREUR had not established a formal Y2K program office; however, MARFOREUR was taking action to address and resolve Y2K issues. The "Headquarters, U.S. Marine Corps Forces Europe Year 2000 Management Plan" (the Plan), August 1998, documents the overall strategy and actions necessary to minimize system failures due to the Y2K problem and to ensure that proper contingency planning is performed. The Plan assigns the MARFOREUR Assistant Chief of Staff, Communications, with the responsibility for overseeing the progress of the subordinate commands; however, each subordinate command is responsible for implementing the Plan. The Plan tasks MARFOREUR subordinate commands to:

- identify and prioritize mission-critical systems in support of local commanders,

³A flexible administrative and tactical unit composed of two or more squadrons.

-
- discontinue or replace application systems as needed,
 - monitor Y2K corrections for systems under their control,
 - make resource decisions and develop strategies for systems with Y2K problems,
 - purchase and develop only Y2K-compliant systems,
 - include Y2K-compliant language in all new contracts and contract modifications, and
 - submit monthly status reports to include an overall appraisal, major concerns, and recommendations.

The MARFOREUR commander is also the commander of U.S. Marine Forces Atlantic and U.S. Marine Forces South. MARFOREUR submits Y2K status information to Marine Corps headquarters, U.S. Marine Forces Atlantic, and USEUCOM. The MARFOREUR Y2K officer stated that a major issue for MARFOREUR was ensuring that Y2K status information obtained from other commands that MARFOREUR relies on for support was current so that MARFOREUR could provide that information to its higher headquarters.

Unit Y2K Readiness Reporting. USEUCOM and its Service Components did not have sufficient information on the Y2K readiness status of units apportioned and assigned to the European theater. For instance, in reviewing the NAVEUR Y2K reporting process, we found that NAVEUR was only reporting on the Y2K status of units and organizations that resided in the theater. Those units and organizations were primarily for support and administration. NAVEUR did not know the Y2K status of warfighting units "chopped" to the command on a rotational basis or the status of permanently assigned TF-67 aviation units⁴ and, consequently, did not include any Y2K status information on those units in its monthly reports to USEUCOM. NAVEUR personnel stated that they were not aware of the Y2K status of combat units in the European theater or how Y2K problems could potentially affect the combat readiness of those units. NAVEUR assumed that the force provider, U.S. Atlantic Command, was working any potential Y2K problems. Also, the NAVEUR Y2K Project Office was not aware of the Y2K status of any warfighting units within the theater. Unless USEUCOM and NAVEUR have oversight of the Y2K status of apportioned and assigned units, there can be no assurance that missions critical to the success of military operations can be successfully carried out. The issue of unit-level Y2K readiness reporting was raised in Inspector General, DoD, Report No. 99-122, "Year 2000 Readiness Reporting," April 2, 1999. If corrective action is taken by the Joint Staff in response to that report, it should assist the unified commands in assessing the Y2K status of assigned or deploying units in theater.

⁴ Air surveillance and reconnaissance unit of P-3 *Orion* aircraft.

Status of Theater Y2K Program Management. Since this audit effort began in September 1998, USEUCOM and its Service Components made significant progress in managing their Y2K programs and continued to be actively involved in resolving Y2K issues. USEUCOM and its Service Components all established command-wide Y2K program offices and transitioned from a systems approach to an operational readiness approach for resolving Y2K issues. That change in approach resulted in active involvement of all levels of USEUCOM and its Service Component staffs in addressing and resolving Y2K issues as issues are identified.

Identification and Prioritization of Mission-Critical Systems

USEUCOM and its Service Components were at various stages of identifying and prioritizing their mission-critical systems. USEUCOM and its Service Components are required to identify and prioritize their mission-critical systems in accordance with the DoD Management Plan. Once all systems are identified and prioritized, USEUCOM should be able to analyze the impact to its operational readiness should priority mission-critical systems not be Y2K compliant.

USEUCOM Mission-Critical Systems. As of September 1998, USEUCOM had not fully identified and prioritized mission-critical systems used in the European theater. USEUCOM had identified the eight mission-critical systems used by USEUCOM headquarters and had a listing of 178 systems that the Service Components stated were used in the European theater; however, that listing had not been analyzed to determine whether the systems were mission-critical and had not been prioritized. In addition, USEUCOM had not analyzed its Joint Mission Essential Task List⁵ to determine the critical tasks and associated critical systems. Also, USEUCOM did not have a process in place to obtain the status of Service and Defense agency mission-critical systems. As of December 1998, the Joint Analysis Center, a division of the USEUCOM Intelligence Directorate, had identified 94 intelligence systems that it used; however, it had not determined which of those systems were mission-critical or prioritized them. Of those 94 systems, 66 were not Y2K compliant. By January 1999, USEUCOM had linked its critical tasks and critical systems to the Joint Mission Essential Task List and was obtaining the Y2K status of mission-critical systems from the DoD Y2K database, its Service Components, and the Joint Analysis Center for use in the operational evaluation.

USAREUR Mission-Critical Systems. The USAREUR headquarters and subordinate commands visited in January 1999 had adequately identified their mission-critical systems. In addition, the subordinate commands had linked their mission-critical systems to their Mission Essential Task Lists. USAREUR headquarters was in the process of completing that same task. USAREUR and its subordinate commands had certified that their unique systems, that were not dependent on DoD and Army standard systems, were Y2K compliant and

⁵A warfighting commander's list of priority tasks, derived from plans and orders, along with associated conditions and measurable standards, constituting the commander's warfighting requirements.

requested that the Army Audit Agency independently verify the Y2K compliance of those unique systems. In addition, USAREUR was tracking the Y2K status of DoD and Army standard systems by searching the Internet, contacting program managers, and looking through available DoD and Army databases. However, USAREUR personnel stated that, because of a lack of a central database within DoD containing all Y2K compliance data, they were spending a substantial amount of time researching the Y2K compliance status of systems.

NAVEUR Mission-Critical Systems. As of October 1998, NAVEUR had not ensured that all its mission-critical systems were identified. Functional users of systems were not involved in the identification or prioritization of critical systems. Instead, the technical staff of the Y2K Project Office identified mission-critical systems. In addition, the Y2K Project Office and functional staffs were not aware of the Y2K status of all systems in use by NAVEUR commands. The NAVEUR memorandum of January 25, 1999, stated that NAVEUR had identified its mission-critical systems and was tracking their Y2K status. In addition, NAVEUR was in the process of prioritizing the non-compliant items and determining which were to be renovated or replaced. Identifying, prioritizing, and monitoring the status of critical systems is necessary for NAVEUR to assess potential Y2K impacts on its operational readiness.

USAFE Mission-Critical Systems. As of December 1998, USAFE had not ensured that all its mission-critical systems were identified. The wings had not identified the Y2K status of aircraft and weapon systems such as the F-15 fighter aircraft and associated systems because a reliable source of information on the Y2K compliance of aircraft and weapon systems was not readily available to wing personnel. In a briefing on January 21, 1999, USAFE provided USEUCOM with a listing of the mission-critical systems for each task on its Mission Essential Task List that needed to be included in the operational evaluation. However, that listing did not include aircraft or weapon systems. Identifying, prioritizing, and monitoring the status of mission-critical systems, including aircraft and weapon systems, will ensure that USAFE has sufficient information to assess potential Y2K impacts on its operational readiness.

Status of Identification and Prioritization of Mission-Critical Systems. During the audit USEUCOM and its Service Components were at various stages of identifying and prioritizing mission-critical systems. Significant progress had been made; however, the lack of an accessible DoD database summarizing the Y2K compliance of DoD systems resulted in the Service Components either not including the information in their Y2K status reports or spending an inordinate amount of time researching data that should be readily available.

Access to the DoD Y2K Database

The Office of the Secretary of Defense Y2K Program Office, an organization within the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), had not disseminated information on how users at the unified commands would obtain training on the new Carnegie Mellon database. In addition, USEUCOM and its Service Components needed to make arrangements for accessing the new database.

DoD Y2K Database. The USEUCOM Y2K Task Force had access to the DoD Y2K database; however, USAREUR and USAFE did not have access to the database and NAVEUR did not use the database. The DoD Y2K database contains information on about 8,000 systems and is accessible on the DoD Secret Internet Protocol Router Network (SIPRNET). The USAREUR Y2K Project Office had used the DoD Y2K database but no longer used it because of the security clearances required for SIPRNET. Although the NAVEUR Y2K Project Office was aware of the DoD Y2K database, it did not use the database because of time constraints. The USAFE Y2K Program Management Office did not have SIPRNET access. The security requirements of SIPRNET restricts some commands' access to the DoD Y2K database.

Carnegie Mellon Y2K Database. The Office of the Secretary of Defense Y2K Program Office recognized the restrictive nature of the DoD Y2K database. As a result, it contracted with the Carnegie Mellon University Software Engineering Institute to develop a new user-friendly Y2K database that would be more accessible. Carnegie Mellon planned to have the new Y2K database operational by mid-March 1999. The Carnegie Mellon database would contain information on the same systems now listed in the DoD Y2K database. In addition, it would track the Y2K progress of those systems through all stages of remediation, certification, and implementation. The Carnegie Mellon database would have password controls and passwords would be provided to system administrators. The system administrators would control access to the database for their assigned areas. The Joint Staff is the systems administrator for the unified commands. However, the Office of the Secretary of Defense Y2K Program Office had not disseminated information on how users at the unified commands would obtain training for the new Carnegie Mellon database. It is not feasible to have all unified command and Service Component users attend the training course in the United States. Therefore, the Office of the Secretary of Defense Y2K Program Office should ensure a users' manual for the new database is made available to prospective users of the Carnegie Mellon database.

USEUCOM and its Service Components need to ensure that they have the specific software requirements needed to access the new database. Specifically, users will be required to have:

- a 128-bit domestic browser with a disabled cache and
- security firewalls that allow the use of:
 - Secure Socket Layer,⁶
 - Cookies,⁷ and
 - unrestricted web browsing.

⁶A web-based technology that lets one computer verify another's identity and allow secure connections.

⁷Small text files stored on the computer by the web site visited.

Without adequate training or a users' manual, and appropriate equipment to access the Carnegie Mellon database, USEUCOM and its Service Components would not be able to use the database for determining the Y2K status of systems in the European theater, or of systems to be fielded in the theater. That information is required for USEUCOM to plan for its operational evaluation.

Status of Access to Y2K Systems Information. The DoD Y2K database is not accessible by all USEUCOM Service Components. The issue of a reliable database for tracking, monitoring, reporting, and overseeing DoD Y2K efforts was addressed in Inspector General, DoD, Report No. 98-169, "Year 2000 Computing Problem Reports: Lessons Learned From the Defense Integration Support Tools Database," June 29, 1998, and numerous other audit agency reports. The Carnegie Mellon database should assist USEUCOM and its Service Components in identifying mission-critical systems and assessing the status of systems, provided USEUCOM and its Service Components make arrangements for access to the new database. In addition, the Office of the Secretary of Defense Y2K Program Office should provide a users' manual to assist users at the unified commands in accessing the Carnegie Mellon database.

Architectures and Configuration Management

System Architectures. USEUCOM and its Service Components had not completed system architectures to determine the Y2K status of its systems. As of September 1998, USEUCOM had not required the development of system architectures⁸ for all functional areas. Developing and analyzing system architectures guarantees functional staff involvement in the Y2K solution. Architectures clearly bring out potential weaknesses in the major elements of functional areas. In addition, they provide a valuable tool for identifying system interfaces, high-risk areas, and potential problems in specific thin-line of systems used to perform functional tasks. Although the Joint Analysis Center had developed a system architecture for the intelligence functional area and the 5th Signal Command had developed system architectures for installation-level, strategic, and tactical communications in the European theater, those were the only system architectures in evidence in the theater. A November 24, 1998, message from the Joint Staff required that all unified commands develop system and operational architectures⁹ for the Joint Staff deconfliction conference that was to be held December 1998. At that conference, USEUCOM provided its operational architectures, but was unable to provide system architectures for all its functional areas. In a January 9, 1999, message, USEUCOM directed that its Service Components provide system architectures at the February 1999 USEUCOM operational evaluation mid-planning conference.

⁸ A system architecture graphically depicts the interconnection of systems, system components, and their associated interfaces within and between operational elements. The graphic may be broken down by tasks or sub-tasks.

⁹ An operational architecture is a graphical depiction of operational elements (functional organizations) supporting the operational concepts or a graphical depiction of geographical configuration and connectivity.

Configuration Management. The Office of the Secretary of Defense Y2K Program Office had not issued policy on configuration management that states the roles and responsibilities of unified commands in addressing configuration management Y2K issues. USEUCOM and its Service Components had not assessed the risk of establishing a moratorium on system changes during the last 3 months of calendar year 1999. USEUCOM recognized that fielding software in the third and fourth quarters of FY 1999 could potentially impact Y2K readiness within the theater. The DoD Management Plan does not require DoD organizations to establish a cut-off date for fielding new software or software upgrades. It does, however, recommend that DoD organizations establish rigorous configuration management procedures to ensure that system modifications do not invalidate the functional and operational testing that has been completed. In addition, the DoD Management Plan recommends that the Services, Defense agencies, unified commands, and Principal Staff Assistants consider a moratorium on changes in the last 3 months of calendar year 1999. However, the DoD Management Plan does not state the ability of unified commands to influence the fielding of software upgrades once a thin-line of systems has been certified as Y2K compliant.

Fielding software upgrades to systems that have been certified as Y2K compliant can cause those systems to no longer be Y2K compliant or may require recertification of Y2K compliance. Although unified commands can unilaterally decline the fielding of new or upgraded systems, by doing so they run the risk of adversely impacting their operational readiness and of losing their interoperability with other unified commands. Fielding new or upgraded systems into a configuration that has been tested, certified as Y2K compliant, and functions properly in an operational environment creates the risk that the new systems will not function properly and may cause systems that were Y2K compliant to no longer be Y2K compliant. USEUCOM had not assessed the risk of fielding new or upgraded systems into a stable Y2K configuration.

Fielding of Migratory Systems. The Joint Analysis Center expressed concerns over delays in the fielding of migratory systems. Several of the migratory systems to be fielded at the Joint Analysis Center are imagery systems. The National Imagery and Mapping Agency, which is responsible for developing several of those systems, scheduled the fielding of several imagery systems, including Imagery Product Library and National Imagery and Mapping Agency Exploitation System, for the third and fourth quarters of FY 1999. However, the Joint Analysis Center was concerned that the systems would not be fielded in time to integrate them into the network and ensure that the systems function as expected in an operational environment. In addition, fielding dates for some of those systems had already slipped by 3 to 6 months.

The timely integration of migratory systems is critical to the Joint Analysis Center's efforts to provide seamless intelligence support to operational forces. The Joint Analysis Center is faced with the fielding of several new systems in the third and fourth quarters of FY 1999. Because of the potential for the late fielding of migratory systems to interfere with day-to-day operations and functional systems already in place, the Joint Analysis Center intends to impose a baseline freeze and accept no new systems from July 1999 to April 2000. Freezes in other functional areas are not anticipated, even though the late fielding of migratory systems could potentially impede a functional area's ability to execute its mission.

Theater Battle Management Core System. Anticipated delays in fully implementing the Theater Battle Management Core System could seriously impair the ability of USEUCOM and its Service Components to carry out their wartime missions. The other combatant commands have similar concerns, as indicated in Inspector General, DoD, Report No. 99-141, "Year 2000 Issues Within U.S. Central Command and the Service Components," April 22, 1999. During FY 1999, the Theater Battle Management Core System is scheduled to replace the Contingency Tactical Automated Planning System, which is not Y2K compliant. That system is used by joint forces to produce air tasking orders, which facilitate much of the day-to-day request and scheduling activities for joint air operations. Accurate and timely air tasking orders are critical to the effective and efficient employment of joint air capabilities in support of operational requirements. According to joint doctrine, joint force Components conduct their planning and operations based on prompt and executable joint air tasking orders and are dependent on their information. Further, the Contingency Tactical Automated Planning System uses the air tasking order generation and dissemination software that allows joint force air operations centers to be interoperable with other force-level Service command and control systems.

Delivery of the Theater Battle Management Core System and its full operational implementation in the European theater is scheduled for October 1999. There is concern at USAFE that delayed delivery dates will not allow sufficient time to integrate the system into USAFE headquarters and subordinate commands. USAFE will not have the opportunity to use the Theater Battle Management Core System in a major joint air operations center exercise before the Contingency Tactical Automated Planning System is due to be replaced. If the current milestones for fielding and implementation of the Theater Battle Management Core System are not met and if the users do not receive standardized guidance for executing contingency efforts, the critical mission of supporting joint air operations would be jeopardized. The problem was briefed to the DoD Y2K Steering Group in January 1999.

Status of Architectures and Configuration Management. The development of system architectures provides a valuable tool for identifying interfaces with standard systems and identifying systems that potentially could impede USEUCOM and its Service Components from executing their mission. It is incumbent upon system program managers to provide standard systems that are Y2K compliant. USEUCOM and its Service Components are reliant on system program managers to field Y2K-compliant systems as soon as possible. While it is possible for USEUCOM to impose a moratorium on the fielding of new or upgraded systems during the last 3 months of calendar year 1999, doing so creates the risk of degrading the unified command's operational readiness. USEUCOM and its Service Components need to complete system architectures and assess the risk of establishing a moratorium on system changes during the last 3 months of calendar year 1999 versus fielding potentially unreliable systems. In addition, the Office of the Secretary of Defense Y2K Program Office should issue policy on the roles and responsibilities of unified commands in addressing configuration management Y2K issues.

Health Care Functional Area

USEUCOM did not include a medical representative from the Command Surgeon's office on the USEUCOM Y2K Task Force. In addition, USEUCOM did not have real-time information needed to adequately report on the Y2K status of DoD health care in the European theater.

Health Care Y2K Reporting Structure. Representation from the Command Surgeon's office on the USEUCOM Y2K Task Force was needed to provide information on the Y2K status of health care. The Y2K status of health care in Europe is reported through the commands responsible for managing health care Y2K efforts. The OASD(HA) and the Military Department medical commands are responsible for DoD health care Y2K efforts, which are divided into three areas: automated information systems, biomedical devices, and facility devices. The OASD(HA) Y2K Project Office centrally manages Y2K efforts over health care information systems. The Military Departments were responsible for the Y2K efforts over biomedical and facility devices, and they had delegated responsibility to the Army Medical Command, the Navy's Bureau of Medicine and Surgery, and the Air Force Medical Support Agency. In addition, a tri-service process action team was established with representation from each of the Military Department medical commands for the biomedical device Y2K effort. Because of the various medical commands and offices involved in monitoring the Y2K status of DoD health care in the European theater, an active medical representative from the Command Surgeon's office is required on the USEUCOM Y2K Task Force.

Automated Information Systems. The Office of the Command Surgeon at USEUCOM identified its critical missions as patient regulating and aeromedical evacuation, medical logistics, and patient blood supply and had identified the critical systems that supported those missions. In addition, the OASD(HA) Y2K Project Office had prioritized the health care systems for DoD and classified 13 systems as mission-critical. However, the Office of the Command Surgeon at USEUCOM did not have real-time access to Y2K status information on patient regulating and aeromedical evacuation systems, biomedical devices, and facility devices, and was unaware that the DoD Y2K database contained Y2K status information on medical logistics and patient blood supply systems.

Patient Regulating and Aeromedical Evacuation Systems. The systems that support patient regulating and aeromedical evacuation in the European theater were not on the OASD(HA) list of mission-critical systems and, therefore, were not in the DoD Y2K database. In December 1998, the responsibility for reporting the Y2K status of the systems used in the European theater for patient regulating and aeromedical evacuation shifted from OASD(HA) to the U.S. Transportation Command. Those information systems are the Defense Medical Regulating Information System and the Automated Patient Evacuation System. In September 1998, the Office of the Command Surgeon at USEUCOM contacted the OASD(HA), but was unsuccessful in obtaining Y2K status information on those two systems. However, the Office of the Command Surgeon later contacted the USAFE Theater Patient Movement Requirements Center and was told that the Defense Medical Regulating Information System and the Automated Patient Evacuation System would not be Y2K compliant until July 1999.

Medical Logistics and Patient Blood Supply Systems. The OASD(HA) is managing Y2K efforts for medical logistics and patient blood supply information systems. The Y2K status for those systems are contained on the DoD Y2K Database; however, the Office of the Command Surgeon at USEUCOM was unaware that they were on the database. In September 1998 the Office of the Command Surgeon requested that the OASD (HA) Y2K Project Office provide information on the Y2K status of the medical logistics and patient blood supply information systems. As of January 1999, the OASD(HA) had not responded to that request. The information systems for medical logistics include Medical Logistics, Theater Army Medical Management Information System – Medical Supply, and the Defense Medical Logistics Support System. The information systems for patient blood supply include the Defense Blood Standard System and the Theater Defense Blood Standard System. On February 1, 1999, the OASD(HA) Y2K Project Office reported that the Medical Logistics system, the Theater Army Medical Management Information System – Medical Supply, and the Defense Medical Logistics Support System were Y2K compliant and implemented. The OASD(HA) Y2K Project Office reported that the Defense Blood Standard System and the Theater Defense Blood Standard System completed implementation on February 19, 1999. The OASD(HA) projected that end-to-end testing would be completed for mission-critical information systems in June 1999. In addition, the OASD(HA) issued Y2K-specific contingency planning guidance for mission-critical information systems.

Biomedical Devices. The medical treatment facilities (MTFs) in Europe reported the Y2K status of biomedical devices (such as a heart monitor) through their Military Departments' medical commands rather than through operational commands. Because the Office of the Command Surgeon at USEUCOM is not part of the reporting process for the Military Department medical commands, it did not have real-time access to information needed to report on the Y2K status of biomedical devices in Europe. Table 1 shows the Y2K status of biomedical devices in the European theater as of January 31, 1999.

Table 1. Y2K Status of Biomedical Devices at MTFs in the European Theater

	<u>Items Inventoried</u>	<u>Y2K Compliant</u>	<u>Non- Complaint, but Upgradeable</u>	<u>Non- Compliant, Must Replace</u>	<u>Non- Compliant, Not Replacing</u>	<u>Awaiting Vendor Response</u>
Army	12,406	12,127	171	9	2	97
Navy	1,180	1,076	97	1	0	6
Air Force	<u>15,855</u>	<u>15,643</u>	<u>180</u>	<u>29</u>	<u>0</u>	<u>3</u>
Total	29,441	28,846	448	39	2	106

The Military Departments had begun to replace non-compliant biomedical devices and were completing the assessment of those biomedical devices that the manufacturer had not responded to Y2K inquiries or the manufacturer had not provided an adequate response. Some manufacturers responded that their devices were not compliant and promised to provide upgrades; however, the manufacturers had not provided a time frame as to when the upgrades would be available or an estimated cost. Priority was being given to follow up on biomedical devices to determine their compliance status and to estimate the cost to repair or replace non-compliant devices. In addition, the tri-service process action team was developing contingency planning and continuity of operations guidance in the event a particular biomedical device fails. Also, the MTFs in Europe were developing detailed continuity of operations plans for patient treatment in the event that a particular biomedical device fails.

Facility Devices. The MTFs in Europe reported the Y2K status of facility devices (such as heating and air conditioning control panels) through their Military Departments' medical commands. Again, the Office of the Command Surgeon at USEUCOM did not have real-time access to information needed to report on the Y2K status of facility devices in Europe. The Military Departments inventoried and assessed facility devices at MTFs and had begun to repair and replace some non-compliant facility devices. Table 2 shows the status of facility devices/systems in the European theater as of January 31, 1999.

Table 2. Y2K Status of Facility Devices/Systems at MTFs in the European Theater

	<u>Devices/ Systems* Inventoried</u>	<u>Y2K Compliant</u>	<u>Non- Complaint, but Upgradeable</u>	<u>Non- Compliant, Must Replace</u>	<u>Non- Compliant, Not Replacing</u>	<u>Awaiting Vendor Response</u>
Army	3,425	3,198	3	0	0	224
Navy	115	45	0	0	0	70
Air Force	<u>74</u>	<u>59</u>	<u>2</u>	<u>0</u>	<u>0</u>	<u>13</u>
Total	3,614	3,302	5	0	0	307

*The Army reported the number of facility devices; the Navy and the Air Force reported the number of facility systems. A facility system can include several facility devices.

The assessment results showed very few non-compliant facility devices at the MTFs in Europe, partly because the facilities are relatively old and most of the facility devices do not contain embedded chips. However, similar to biomedical devices, some manufacturers either had not responded or had not provided adequate response to DoD inquiries. The Military Department medical commands provided contingency planning and continuity of operations guidance to MTFs, and MTFs in the European theater were in the early stages of developing contingency plans and continuity of operations plans.

Status of the Health Care Functional Area. Y2K efforts for DoD health care were ongoing and generally successful, as reported in Inspector General, DoD, Report No. 99-055, "Year 2000 Computing Issues Related to Health Care in DoD," December 15, 1998. Although DoD health care is not a USEUCOM responsibility, USEUCOM should be aware of the Y2K readiness of health care within the European theater. To gain visibility over the Y2K readiness of health care in its area of responsibility, USEUCOM needs to coordinate with the Military Department medical commands, the OASD(HA), and the U.S. Transportation Command to obtain Y2K status information. In addition, USEUCOM should include a representative from the USEUCOM Command Surgeon's office on the USEUCOM Y2K Task Force.

Operational Contingency Planning

USEUCOM and its Services Components had not uniformly developed operational contingency plans for missions that may be affected by the Y2K problem. The DoD Management Plan states that:

Y2K Operational CPs [contingency plans] identify alternative system(s) or procedures (work-arounds) to use when performing a mission or function, in the event a primary system is disrupted. Commanding Officers (Operational, Support, Base/Facility) and Civilian Directors shall document alternative systems and procedures in their Operational CP in order for them to be able to sustain the minimum operational capabilities required to support our national military strategy. Y2K Operational CPs shall address all systems required by that operational commander to perform his/her mission(s) or functional responsibility.

The DoD Management Plan distinguishes between an operational contingency plan and a continuity of operations plan.

The term COOP [continuity of operations plan] refers to plans initiated by an executive order in 1988. DoDD [DoD Directive] 3020.26, *Continuity of Operations Policy and Planning* requires echelon II and above commands to develop COOPs to ensure continuity of mission critical and mission essential operations during an impending or actual national emergency. (Y2K Contingency Plans labeled as COOPs are generally Operational Contingency Plans and do not have to change their name.) *This management plan does not require COOPs as defined by the DoD Directive to be developed.* However, when such COOPs already exist, it may be appropriate for that plan to be used in lieu of a Y2K Operational CP for the missions and functions supported by the COOP plan. COOPs may serve as Y2K Operational CPs as long as the COOP is made "Y2K aware" by updating its content, or adding a Y2K appendix, to reflect a recovery strategy and plan that addresses disruptions caused by Y2K.

The DoD Management Plan states that operational contingency plans deal with continuing and completing missions and functions in "worst case" scenarios. Each core mission and function and critical process should have an operational contingency plan. A continuity of operations plan is developed to ensure the continuity of a mission-critical or mission-essential operation during an impending or actual emergency. Each core mission and function should have an

operational contingency plan. The DoD Management Plan requires that operational contingency plans be completed by March 31, 1999, and be exercised by June 30, 1999.

USEUCOM Planning. As of January 1999, USEUCOM was not developing operational contingency plans. The USEUCOM Y2K Task Force intended to use the operational evaluation as a mechanism to discover which critical missions needed operational contingency plans and then develop operational contingency plans for those functional areas requiring alternative procedures because of Y2K failures during the evaluation. However, it is necessary to have the operational contingency plans prepared in advance so that they can be tested during the operational evaluation to determine whether the alternative procedures are viable. In addition, the DoD Management Plan requires that all operational contingency plans be tested by June 30, 1999. If USEUCOM waits until after the operational evaluation, scheduled for May 1999, it may not have enough time to test the plans before June 30, 1999.

USAREUR Planning. As of January 1999, USAREUR was in the process of developing operational contingency plans for its missions that might be affected by the Y2K problem. USAREUR had considered the potential impact on its ability to execute its critical missions and functions should systems fail as a result of Y2K problems. USAREUR had finished the system contingency plans for its unique systems and was working on operational contingency plans. USAREUR expected to have its operational contingency plans completed in time for the USEUCOM operational evaluation in May 1999. USAREUR estimated that it would complete its operational contingency plans for facilities infrastructure by the summer of 1999. The "U.S. Army Year 2000 (Y2K) Action Plan," Revision II, June 1998, and the Army Y2K home page on the Internet, maintained by the Army Y2K Program Office, provided limited guidance on the preparation of operational contingency plans. Although USAREUR was achieving significant progress, USAREUR was using guidance from other sites on the Internet and from other organizations as a basis for developing its plans. For example, the 104th Area Support Group was developing operational contingency plans for its facilities infrastructure partially based on information obtained from the Internet, including the city of Cleveland's contingency plan. The Army Y2K Program Office needs to issue operational contingency planning guidance so that USAREUR and its subordinate commands have standardized guidance instead of relying on unofficial guidance provided by unofficial sources.

NAVEUR Planning. As of October 1998, NAVEUR had not developed operational contingency plans for missions that might be affected by the Y2K problem. Functional staffs were waiting for system program managers to provide system contingency plans before developing operational contingency plans. NAVEUR and its subordinate commands needed to take the steps necessary to develop operational contingency plans before the start of the USEUCOM operational evaluations. However, there was very little Navy guidance on the development of those plans until the Navy Y2K Project Office issued "Navy Y2K Contingency & Continuity of Operations Planning Guide," November 1, 1998. That guide provides a comprehensive description of the information to be included in Y2K contingency plans for all Navy organizations ashore and afloat. The guide includes templates for plans and examples of completed plans. Since the guide's publication, NAVEUR made substantial progress in developing

operational contingency plans. The NAVEUR memorandum of January 25, 1999, states that it had developed 85 of 88 required continuity of operations plans for mission-critical functions, including facilities; maintenance; and command, control, communications, and computer systems. The three remaining plans were completed by January 31, 1999.

USAFE Planning. As of December 1998, USAFE was proactively developing operational contingency plan and continuity of operations plans and expected to complete them by mid-March. Air Force major commands, numbered air forces, and wings are required to develop continuity of operations plans in accordance with Air Force Instruction 10-232, "Year 2000 Continuity of Operations," September 3, 1998, and Air Force Instruction 10-208, "Continuity of Operations Plans," July 1, 1995. Additionally, the Air Force had designated Y2K accountability as a special interest item. Each command is required to complete a self-inspection checklist that includes the status of contingency planning. In January 1999, the USAFE Inspector General began conducting field inspections to validate the results reported in the self-inspection checklists.

Status of Operational Contingency Planning. USEUCOM was not developing operational contingency plans, opting instead to wait for the results of the operational evaluation to use as the basis for operational contingency planning. USEUCOM should not wait until the operational evaluation before developing its operational contingency plans because its plans should be tested during the operational evaluation. The Service Components made substantial progress in developing operational contingency plans that they expected to test during the operational evaluation, even though the Army Y2K Program Office had not provided standardized operational contingency planning guidance and the Navy Y2K Project Office did not issue guidance until November 1998. All contingency plans for the European theater needed to be completed no later than March 31, 1999, to conform with the DoD Management Plan.

Operational Evaluation Planning

USEUCOM was making progress in planning for its operational evaluation. Inclusion of aircraft and weapon systems and NATO participation will improve the effectiveness of the operational evaluation.

Critical Missions to be Evaluated. At the September 1998 Joint Staff Operational Evaluation conference, the Joint Staff tasked USEUCOM to perform an operational evaluation on its critical missions of non-combatant evacuation operations¹⁰ and peacekeeping operations. The objective of the operational evaluation is to verify that a unified command can successfully perform its missions, functions, and tasks in a Y2K environment.

¹⁰ A non-combatant evacuation operation is conducted to safely and quickly remove civilians from an area outside the United States where they are, or might be, threatened.

As of September 1998, USEUCOM had not begun to prepare the operational evaluation plan for its assigned missions. At that time, USEUCOM expressed concern that it did not have enough technical expertise in the theater to write an operational evaluation plan, conduct the evaluation, and analyze the results. However, by January 1999, USEUCOM had hired a contractor to prepare a single operational evaluation plan for both missions and had met with the Joint Staff, other unified commands, and the USEUCOM Service Components to initiate the operational evaluation planning process.

Operational Evaluation Plan. An operational evaluation plan dated March 22, 1999, provides planning, execution, and evaluation information and instructions for the USEUCOM operational evaluation. The plan breaks up the operational evaluation into six phases: pre-evaluation systems check, rehearsal, actual evaluation, restoration, results reporting, and followup. USEUCOM objectives for the operational evaluation are to:

- ensure that critical missions and tasks can be accomplished in a Y2K environment,
- ensure that the USEUCOM thin-line of critical systems correctly process information in the Y2K environment, and
- ensure development and evaluation of necessary contingency plans to work through identified Y2K problems and demonstrate the ability to accomplish needed tasks using those plans.

The USEUCOM operational evaluation will test the flow of information from joint systems to major Service Component systems. According to USEUCOM, the Service Components can decide whether to test from their major systems down to Service-unique systems during the operational evaluation. However, the operational evaluation will not evaluate an integrated joint or combined force structure.

Integrated Force Structure. USEUCOM does not plan to test aircraft or weapon systems (to include the M1A2 tank) during its operational evaluation. Non-combatant evacuation operations and peacekeeping operations require the integration of forces from at least two Military Departments. USEUCOM officials stated that they were relying on the Military Departments to test aircraft and weapon systems during the Military Department operational evaluations. However, testing by one Military Department of its weapon systems does not validate the ability of those systems to operate across the Military Departments in an integrated force structure. USEUCOM should ensure that all systems used to accomplish non-combatant evacuation operations and peacekeeping operations are tested within an integrated force structure.

Testing Peacekeeping Operations as a Combined Force. USEUCOM does not plan to conduct the peacekeeping portion of the operational evaluation with NATO (see Appendix G for the status of the NATO Y2K program). A peacekeeping operation is a noncombat military operation conducted to enforce or maintain a peaceful settlement among belligerent parties. Peacekeeping operations usually include combined military forces from several countries or international organizations. For example, the NATO-led Stabilization Force

deployed in Bosnia-Herzegovina, with the mission to achieve a secure environment to ensure peace in the region, is a peacekeeping operation. USEUCOM supports the operation by providing the headquarters and most of the troops for one of the three NATO-led multinational divisions. USEUCOM also provides equipment, personnel, and units to various parts of the Stabilization Force. Because peacekeeping operations in the European theater usually include NATO forces, USEUCOM should invite NATO to participate in the peacekeeping portion of the operational evaluation.

Status of USEUCOM Operational Evaluation. USEUCOM was making progress in planning for its operational evaluation. However, USEUCOM may not be able to fully assess its ability to perform its critical missions of non-combatant evacuation operations and peacekeeping operations because USEUCOM was not planning to include aircraft and weapon systems as part of the evaluation or to invite NATO to participate in the peacekeeping portion. Without including aircraft and weapon systems or inviting NATO to participate in the peacekeeping portion of the evaluation, USEUCOM cannot fully evaluate the integrated force structure that it would implement during an operation and, thus, the planned operational evaluation will not provide a complete assessment of the USEUCOM operational readiness in a Y2K environment.

Facilities and Host Nation Infrastructure

USEUCOM and its Service Components identified facilities infrastructure¹¹ and host nation infrastructure¹² as major problem areas in the European theater. As of January 1999, Service Components were completing facilities infrastructure inventories and actively repairing and replacing all facilities infrastructure items that would be adversely affected by the Y2K problem. However, USEUCOM and its Service Components had no guidance or coherent approach to addressing the host nation infrastructure issue.

Theater Facilities Infrastructure. The USEUCOM Service Components were completing facilities infrastructure inventories and actively repairing and replacing items that could be affected by the Y2K problem.

USAREUR Facilities Infrastructure. The USAREUR Deputy Chief of Staff, Engineer, and the area support groups are responsible for the Y2K compliance of USAREUR facilities infrastructure. That includes the infrastructure used by tenant organizations such as Army airfields, the Defense Commissary Agency, DoD Dependent Schools, MARFOREUR, medical commands, and USEUCOM headquarters. The USAREUR Office of the Deputy Chief of Staff, Engineer, awarded a \$310,000 contract for the inventory and assessment of USAREUR facilities infrastructure in the European theater. The initial inventory and assessment was scheduled for completion by January 29, 1999. USAREUR was also in the process of awarding a contract, with an

¹¹Facilities infrastructure includes elevator controls, emergency power supplies, entry controls, fire alarms, security systems, uninterruptable power supplies, and utility monitoring and control systems.

¹²Host nation infrastructure includes electricity, sewer, telephone service, and water.

estimated value of \$6 million, to validate the inventory and assessment as well as to repair or replace all Y2K non-compliant items that impact its operations. In addition, the contract would include a warranty provision to guarantee that all items will work through and past January 1, 2000. USAREUR awarded the contract on April 19, 1999. USAREUR planned to have all facilities infrastructure items that would be adversely affected by the Y2K problem either repaired or replaced by June 30, 1999.

NAVEUR Facilities Infrastructure. The NAVEUR Deputy Chief of Staff Facilities is responsible for the Y2K compliance of NAVEUR facilities infrastructure. NAVEUR contracted with the Naval Air Warfare Center China Lake to complete a facilities infrastructure inventory and assessment by November 1998. As of October 1998, NAVEUR had identified 217 mission-critical buildings. At that time, the Y2K status of the buildings was unknown. NAVEUR planned to have infrastructure items prioritized for upgrades as necessary by November 30, 1998. In its memorandum of January 25, 1999, NAVEUR stated that its facilities infrastructure inventory and assessment was complete and it anticipated that renovation of non-compliant items would be completed by April 1, 1999, which would be ahead of the schedule in the NAVEUR Y2K Action Plan. The NAVEUR Y2K Action Plan requires that the renovation of mission-critical facilities infrastructure be completed by May 1, 1999, and the renovation of mission-support facilities infrastructure be completed by August 1, 1999.

USAFE Facilities Infrastructure. The USAFE Civil Engineering Squadrons are responsible for the facilities infrastructure on USAFE air bases. As of January 31, 1999, USAFE had completed all inventories, assessments, and contingency plans. The USAFE Civil Engineering Squadron Y2K representatives explained that facilities infrastructure such as airfield traffic lights, electricity, fire alarm and detection systems, and water supply had existing disaster plans that included contingency procedures, impacts of failure, locations, purposes, and system descriptions. The existing plans prioritized responses to base disasters.

Host Nation Infrastructure. USEUCOM and its Service Components had no guidance or coherent approach to addressing the host nation infrastructure issue. In addition, USEUCOM had not established a central point within the Y2K Task Force for obtaining Y2K status information on host nation infrastructure in the European theater. As of January 1999, the USEUCOM Y2K Task Force had not issued any guidance to its Service Components on addressing host nation infrastructure issues. As a result, Service Components and subordinate commands were acting independently to contact local governments and utilities on the matter. For example, the 104th Area Support Group in Hanau, Germany, met with city officials to obtain written certification about the Y2K compliance of commercial electric, sewer, and water facilities. In addition, NAVEUR facilities in Italy and Spain were writing letters requesting confirmation of Y2K compliance. Personnel at RAF Mildenhall, in the United Kingdom, stated that British law requires utilities to be Y2K compliant and that was all that could be done. A USEUCOM Y2K Task Force member stated that the Service Components were receiving sufficient guidance from their higher headquarters and the task force did not see the need to provide additional guidance on addressing host nation infrastructure issues. Because subordinate commands were acting independently and the USEUCOM Y2K Task Force was not obtaining and

assessing data on host nation infrastructure, USEUCOM did not have sufficient information to assess the magnitude of host nation infrastructure Y2K issues.

Status of Facilities Infrastructure and Host Nation Infrastructure. The Service Components of USEUCOM were actively pursuing facilities infrastructure Y2K issues for the European theater. However, additional emphasis was needed in the area of host nation infrastructure Y2K issues. The USEUCOM Y2K Task Force should issue guidance to its Service Components for uniformly addressing host nation infrastructure Y2K issues. In addition, the USEUCOM Y2K Task Force should be the central point for obtaining and maintaining data on host nation infrastructure that might be common among the Service Components to avoid duplication of effort by the Service Components in determining Y2K compliance.

Y2K Funding Requirements

USEUCOM and its Service Components had not fully identified and validated Y2K funding requirements for their Y2K efforts. Although USEUCOM and its Service Components established Y2K offices, the resources to support those offices were acquired from other activities within their respective commands. Funding for USEUCOM Y2K efforts came from its operation and maintenance account. In January 1999, USEUCOM and its Service Components had identified and validated Y2K operational evaluation funding requirements of more than \$3.8 million for FY 1999. In addition, USEUCOM and its Service Components were in the process of identifying other resource requirements needed for their Y2K efforts. Resource requirements identified included the following.

- USAREUR had identified, but not validated, \$10.7 million of funding that was diverted from other projects in FY 1997 and FY 1998 to support Y2K efforts. Specifically, funds were diverted from the planned network installation at the 104th Area Support Group and the Seventh Army used mission funds to replace computers. The Seventh Army stated that using mission funds for Y2K efforts would directly impact its ability to support USAREUR exercises for the next 5 to 7 years.
- USAREUR had identified, but not validated, \$14.5 million of Y2K requirements in FY 1999 for contractor support, new computer hardware, repair and replacement of facilities infrastructure, etc.
- USAREUR had identified, but not validated, \$9.9 million of deferred requirements for FY 1999, mostly for installation of networks and the repair and replacement of facilities infrastructure.
- NAVEUR identified and validated \$11.7 million in unfunded requirements for facilities infrastructure upgrades, replacement of computers, and software. However, not all of the requirements may be

attributable to the Y2K problem. NAVEUR stated that its current hardware was unable to run many of the new software programs because it was obsolete.

- The USAFE 48th Fighter Wing at RAF Lakenheath identified and validated about \$3 million in unfunded Y2K requirements to replace non-compliant hardware and aircraft maintenance equipment such as a tube bender used to make fuel lines, hydraulic lines, and air pressure lines for all types of aircraft throughout the European theater.
- The USAFE 52nd Fighter Wing at Spangdahlem Air Base identified and validated an unfunded \$2.6 million Y2K requirement to replace non-compliant computer hardware.

Status of Y2K Funding Requirements. USEUCOM and its Service Components need to determine what remains to be repaired, replaced, or tested as a result of the Y2K problem to ensure that there is no degradation of their operational readiness. Once a full determination is made of resource requirements, USEUCOM and its Service Components should submit funding requirements to their higher headquarters.

Conclusion

USEUCOM and its Service Components made significant progress in addressing their Y2K problems; however, additional work remained. To avoid undue disruption of its mission, USEUCOM and its Service Components must improve their performance in the limited time remaining before the year 2000. The combination of operational demands on USEUCOM and its Service Components and the limited availability of resources to support Y2K activities, placed significant demands on units tasked with planning and executing joint operations. For example, USEUCOM provides support to NATO in Bosnia-Herzegovina. In addition, USAFE was participating in the combined task force charged with enforcing the no-fly zone in Iraq. The systems that are used in conducting those day-to-day operations cannot be taken off-line to conduct testing and validation of Y2K repairs without putting U.S. forces in the area of responsibility at risk. It is precisely the volatile nature of portions of the USEUCOM area of responsibility, however, that makes it vital for the Command to have an aggressive and fully effective Y2K program to assure continued mission capability.

Recommendations, Management Comments, and Audit Response

Redirected, Added, and Renumbered Recommendations. As the result of USEUCOM comments, we added Recommendation 4.a. to the Joint Staff. In addition, we redirected draft Recommendation 1.h. to the Joint Staff and renumbered it as Recommendation 4.b. We also renumbered draft Recommendations 1.i., 1.j., and 1.k. to Recommendations 1.h., 1.i., and 1.j.

1. We recommend that the Commander in Chief, U.S. European Command, through the Year 2000 Task Force and in coordination with its Service Component year 2000 offices:

a. Ensure that users of the Carnegie Mellon database have the appropriate equipment that allows them to access the database.

USEUCOM Comments. USEUCOM concurred, stating that the Carnegie Mellon database file was being distributed via email to its Service Components and the USEUCOM Y2K Task Force would continue to distribute it via email until it is on line.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Office of the Assistant Secretary stated that the Carnegie Mellon database is accessible via the Internet with a 128-bit domestic browser. If the unified commands do not have the required browser, then they must download it from the Defense Information Systems Agency web site. Any additional access problems to the database will be worked on a case-by-case basis when the Office of the Assistant Secretary is notified that there is a problem.

b. Complete system architectures to determine year 2000 status for all mission-critical functional areas.

USEUCOM Comments. USEUCOM concurred, stating that the current focus of detailed system architectures is in support of the USEUCOM operational evaluation of its critical missions of non-combatant evacuation, peacekeeping, and non-strategic nuclear forces operations. USEUCOM completed detailed system architectures for the mission-critical strategic tasks and the subordinate operational and tactical tasks related to its critical missions. Upon completion of its operational evaluation, USEUCOM will continue to monitor and report on the Y2K status of the 10 functional areas that are not addressed in any of the unified command operational evaluations.

Audit Response. The USEUCOM comments are responsive. Although USEUCOM stated that it had only completed system architectures for the operational evaluation, USEUCOM submitted system architectures for all its mission-critical functions to the Joint Staff via email on March 26, 1999.

c. Assess the risk of establishing a moratorium on system changes during the last 3 months of calendar year 1999 versus fielding potentially unreliable systems.

USEUCOM Comments. USEUCOM concurred, stating that it supported the Joint Staff recommendation that the unified commands have the ultimate authority to grant a waiver to any such moratorium, allowing the flexibility to make or deny changes based on a case-by-case risk assessment. USEUCOM will publish configuration management guidance for all systems in the European theater after the Office of the Secretary of Defense and the Joint Staff publish higher headquarters guidance, which was being developed and staffed.

d. Include representation from the Command Surgeon's office on the U.S. European Command Year 2000 Task Force.

USEUCOM Comments. USEUCOM partially concurred, stating that, due to personnel shortages, the USEUCOM Office of the Command Surgeon was only able to provide a part-time representative to the USEUCOM Y2K Task Force.

Audit Response. The USEUCOM actions meet the intent of the recommendation.

e. Coordinate with the Military Department medical commands, the Office of the Assistant Secretary of Defense (Health Affairs), and the U.S. Transportation Command to obtain the year 2000 status of health care systems used in the theater.

USEUCOM Comments. USEUCOM partially concurred, stating that, since the Inspector General, DoD, visit, the USEUCOM Y2K Task Force medical representative met with the Chief Information Officers for the Service Components in the European theater and requested their support in providing information as it relates to medical Y2K status in the theater. In addition, the medical representative contacted the Joint Staff about how to stay current on Y2K-related medical issues of the OASD(HA) and the U.S. Transportation Command. USEUCOM stated that the Joint Staff agreed to continue providing USEUCOM with that information as it becomes available.

Audit Response. The USEUCOM actions meet the intent of the recommendation. Continued coordination by USEUCOM should result in it having access to information needed to assess the Y2K readiness of health care within the European theater.

f. Prepare all required operational contingency plans by March 31, 1999, as required by the DoD Year 2000 Management Plan, Version 2.0.

USEUCOM Comments. USEUCOM partially concurred, stating that its first priority was preparing operational contingency plans and continuity of operations plans that were required for the operational evaluation. Its second priority was preparing operational contingency plans and continuity of operations plans for the intelligence, reconnaissance, and surveillance functional area for the Joint Staff-run Chairman's Contingency Assessment Positive Response Y2K-3, scheduled for June 1999. Its third priority was to finalize operational contingency plans and continuity of operations plans for systems not addressed in the operational evaluation or the Chairman's Contingency Assessment. USEUCOM estimated that all required operational contingency plans and continuity of operations plans would be completed by September 30, 1999.

Audit Response. Although USEUCOM did not have all its required operational contingency plans and continuity of operations plans prepared by March 31, 1999, as required by the DoD Management Plan, its actions meet the intent of the recommendation. The USEUCOM approach of completing those plans needed for the operational evaluation first and the Chairman's Contingency Assessment second will meet the DoD Management Plan requirement to exercise operational contingency plans and continuity of operations plans for mission-critical

operations by June 30, 1999. Although USEUCOM will not be able to complete the remaining plans until sometime after June 30, 1999, completion of those plans by September 30, 1999, should still provide USEUCOM with sufficient time to test the viability of those plans.

g. Include aircraft and weapon systems in the operational evaluation plan in order to evaluate an integrated force structure.

USEUCOM Comments. USEUCOM partially concurred, stating that the focus of its operational evaluation is mission-critical joint systems, their interfaces with Service systems, and cross-Service systems and interfaces. The Services are conducting robust evaluations of their Service-unique systems, including weapon systems. USEUCOM plans on conducting a complete review of those efforts to ensure that USEUCOM thin-line of systems and critical tasks are evaluated in the Service efforts. A "virtual end-to-end" operational evaluation will then be completed by coupling the USEUCOM-executed operational evaluation with the multiple Service efforts. That will save resources, avoid redundancy, spread the efforts among many participants, and keep the responsibility for system evaluations with the primary owner and users of the systems.

Audit Response. The USEUCOM comments are sufficiently responsive when compared to some of the criteria outlined in the Joint Staff "Year 2000 Operational Evaluation Guide" Version 3.0 (Joint Staff guidance), April 1, 1999. The Joint Staff guidance states:

Operational Evaluation events are designed to evaluate the ability of previously certified Y2K compliant systems to support joint and combined operations from sensor-to-shooter under conditions replicating a Year 2000 environment. . . . The primary objective of the operational evaluation is to validate the information flow for critical missions and tasks using the CINC [Commander in Chief] identified "Thin Line" of critical systems in a Y2K environment. . . . Each CINC is trying to ensure a reliable information flow and infrastructure support is available to support operational requirements! . . . Systems the CINCs may not be able to evaluate based upon real-world operational considerations and limitations [must be] identified. CINCs will simulate these capabilities or use other means (labs/other CINC results) to analyze the risks associated with these systems.

The Joint Staff guidance also states that the operational evaluation planned by the combatant commands may only cover one or two echelons¹³ up and down and that another event may be necessary to provide sufficient overlap of echelons. That contradicts the stated requirement that an operational evaluation is a "sensor-to-shooter" assessment of a combatant command's ability to perform its critical missions in a Y2K environment. Specifically, the Joint Staff guidance states that "the ultimate goal is to assess your capability to carry out the most critical missions without disruption in a Y2K environment." Because of the inconsistencies in the Joint Staff guidance, we have added a recommendation requesting that the Joint Staff modify its guidance to clarify the scope of what the combatant commands are expected to assess during operational evaluations.

¹³An echelon is a separate level of command. As compared with a regiment, a division is a higher echelon, a battalion is a lower echelon.

h. Issue guidance for uniformly addressing host nation infrastructure issues.

i. Establish a central point within the European theater for maintaining year 2000 compliance data on host nation infrastructure.

USEUCOM Comments. USEUCOM concurred with the recommendations, stating that the USEUCOM Y2K Task Force is the central office for European theater host nation issues. In addition, the task force has a draft plan to be published in August 1999 to formally provide direction and oversight for European theater host nation issues. The Service Components, at the direction of their higher Service headquarters, have robust programs for host nation interactions, infrastructure validation, and contingencies. USEUCOM monitors Service Component preparedness in this area through the monthly report, where infrastructure is one of the nine functional areas that each Service Component is required to report on.

j. Identify and validate year 2000 funding requirements.

USEUCOM Comments. USEUCOM concurred, stating it had received funding from the Joint Staff to support the Y2K efforts in the European theater.

2. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

a. Issue and disseminate a users' manual to the unified commands for the Carnegie Mellon database.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Office of the Assistant Secretary stated that it provided the Joint Staff with users' manuals for the Carnegie Mellon database and information on how users at the unified commands could obtain training on using the database. The Office of the Assistant Secretary pointed out that the Joint Staff, as the administrator for the unified commands, is responsible for forwarding guidance to the unified commands. However, the Office of the Assistant Secretary has requested that the Joint Staff provide points of contact at the unified commands so that the Office of the Assistant Secretary can deal directly with the unified commands in the future.

Audit Response. The Office of the Assistant Secretary actions meet the intent of the recommendation.

b. Issue policy on the roles and responsibilities of unified commands in addressing configuration management year 2000 issues.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Office of the Assistant Secretary stated that the Office of the Secretary of Defense Y2K Program Office was working on a configuration management policy for DoD Y2K systems to ensure that all DoD software development and software maintenance programs have established procedures. The Office of the Assistant Secretary stated that the Y2K-compliant

version of a system, which would have been established upon completion of the five-phase program, should be used for operational evaluations or functional end-to-end testing.

Audit Response. The Office of the Assistant Secretary comments were generally responsive. The Office of the Assistant Secretary needs to take into account that many systems were not Y2K compliant by the deadlines specified in the five-phase program: December 31, 1998, for mission-critical systems and March 31, 1999, for non-mission-critical systems. Any configuration management policy must recognize that not all mission-critical systems will be Y2K compliant in time for operational evaluations and functional end-to-end testing. We request that the Office of the Assistant Secretary provide additional information on the details of its configuration management policy and an implementation date in response to the final report.

3. We recommend that the Army Year 2000 Program Office issue operational contingency planning guidance.

Management Comments. The Army concurred, stating that the Army Y2K Program Office is in the process of updating the contingency planning section of the Army Y2K home page to include more guidance on operational contingency planning. In addition, the Army Chief Information Officer is issuing a Y2K policy update to all Army organizations that includes guidance on both system and operational contingency planning. Both efforts were to be completed in March 1999.

4. We recommend that the Director, Joint Staff:

a. Modify the "Year 2000 Operational Evaluation Guide," Version 3.0, April 1, 1999, to clarify the scope of the operational evaluations.

b. Initiate action to invite the North Atlantic Treaty Organization to participate in the peacekeeping portion of the U.S. European Command operational evaluation.

USEUCOM Comments. USEUCOM partially concurred with Recommendation 4.b. which was directed to USEUCOM in the draft report. USEUCOM stated that its operational evaluation will only involve U.S. systems. USEUCOM recognized the importance of NATO in support of U.S. interests; however, USEUCOM cannot ensure that allied nation and coalition partner systems are operationally evaluated. USEUCOM suggested that an initiative to include NATO come from either the Office of the Secretary of Defense or the Joint Staff. USEUCOM is in the process of identifying all possible current and planned interfaces between U.S. and allied nation systems and reporting them to the Joint Staff and is meeting with Supreme Headquarters Allied Powers Europe on Y2K issues through the U.S. National Military Representative.

Audit Response. Although USEUCOM only partially concurred, we consider its comments responsive. As a result of the USEUCOM comments, we redirected draft report Recommendation 1.h. to the Joint Staff. We request that the Joint Staff provide comments on the final report.

Appendix A. Audit Process

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge.

Scope

We reviewed and evaluated the ability of USEUCOM and its Service Components to resolve Y2K issues to avoid undue disruption of its mission. We reviewed and evaluated DoD, Service, and Joint Staff directives, policies, and processes related to Y2K activities dated from September 1997 through January 1999. We also reviewed issues related to DoD Y2K database access, architectures, configuration management, the Theater Battle Management Core System, health care, operational contingency planning, operational evaluation planning, facilities and host nation infrastructure, and Y2K funding.

For this report we visited various organizations within the European theater. We visited USEUCOM headquarters, Stuttgart, Germany, and the Joint Analysis Center, RAF Molesworth, United Kingdom. For the Army Service Component, we visited USAREUR headquarters, Heidelberg, Germany; 21st Theater Army Area Command, Kaiserslautern, Germany; 5th Signal Command; 1st Personnel Command and 266th Finance Command, Heidelberg, Germany; 104th Area Support Group, Hanau, Germany; and the 66th Military Intelligence Group, Darmstadt, Germany. For the Navy Service Component, we visited NAVEUR headquarters, London, United Kingdom; Fleet Air Mediterranean, Naples, Italy; and Naval Support Activity Naples, Italy. For the Air Force Service Component, we visited USAFE headquarters, Ramstein Air Base, Germany; 48th Fighter Wing, RAF Lakenheath, United Kingdom; 31st Fighter Wing, Aviano Air Base, Italy; and 52nd Fighter Wing, Spangdahlem Air Base, Germany. To evaluate the health care functional area, we visited the Office of the Command Surgeon at USEUCOM and six MTFs, located at Aviano Air Base, Italy; Heidelberg, Germany; RAF Lakenheath, United Kingdom; Landstuhl Regional Medical Center, Germany; Naval Support Activity Naples, Italy; and Spangdahlem Air Base, Germany.

DoD-Wide Corporate Level Goals. In response to the Government Performance and Results Act, DoD has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities. (DoD-3)
- **Objective:** Maintain highly ready joint forces to perform the full spectrum of military activities. **Goal:** Maintain high military personnel and unit readiness. (DoD-5.1)

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following objectives and goals in the Information Management Functional Area.

- **Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. (ITM-1.2)
- **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. (ITM-2.2)
- **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. (ITM-2.3)

High Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Methodology

We focused our review of USEUCOM on the Y2K efforts of the unified command headquarters and its Service Components. We assessed the progress of USEUCOM since the most recent Army Audit Agency review of the unified command's Y2K issues. We reviewed the process employed by USEUCOM and its Service Components to identify and prioritize mission-critical systems and to develop operational contingency plans. To determine the Y2K status of the Service Components, we reviewed their respective criteria and processes for identifying and reporting Y2K compliance. We interviewed the leadership and members of the Y2K entities established at USEUCOM and its Service Components. We also interviewed members of the unified command and Service Component staffs to determine the respective command's level of involvement and interest in addressing Y2K problems; to determine their ability to access the DoD Y2K database; to assess the Y2K impact on joint force architectures; to evaluate the impact on the commands caused by the delay in fielding DoD standard systems; to identify any mission-critical systems not previously considered; to assess the status of host nation Y2K efforts; and to review the funding requirements of the commands. We reviewed the impact and influence of supporting commands on USEUCOM Y2K compliance and testing efforts. We did not use computer-processed data to perform this audit.

Audit Type, Dates, and Standards. We performed this program audit from September 1998 through March 1999 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at <http://www.gao.gov>. Inspector General, DoD, reports can be accessed over the Internet at <http://www.dodig.osd.mil>. The following previous reports are of particular relevance to the subject matter in this report.

Inspector General, DoD

Report No. 99-141, "Year 2000 Issues Within U.S. Central Command and the Service Components," April 22, 1999.

Report No. 99-122, "Year 2000 Readiness Reporting," April 2, 1999.

Report No. 99-059, "Summary of DoD Year 2000 Conversion – Audit and Inspection Results," December 24, 1998.

Report No. 99-055, "Year 2000 Computing Issues Related to Health Care in DoD," December 15, 1998.

Report No. 98-169, "DoD Year 2000 Computing Problem Reports: Lessons Learned from the Defense Integration Support Tools Database," June 29, 1998.

Report No. 98-077, "Year 2000 Computing Problem Report: August 1997 Report," February 18, 1998.

Report No. 98-074, "Sharing Year 2000 Testing Information on DoD Information Technology Systems," February 12, 1998.

Army Audit Agency

Memorandum Report No. AA 98-292, "U.S. European Command's Management of the Year 2000," July 30, 1998.

Appendix C. Office of the Secretary of Defense Memorandums

The Secretary of Defense and the Deputy Secretary of Defense have issued two particularly significant memorandums on DoD Y2K efforts.

Y2K Compliance. The Secretary of Defense issued a memorandum, "Year 2000 Compliance," on August 7, 1998, which asserted that DoD was making insufficient progress on Y2K conversion. He directed a number of actions, including the following.

- The Joint Chiefs of Staff was to develop a Joint Y2K operational evaluation program and to provide the plans to the Secretary of Defense by October 1, 1998.
- The unified commanders in chief were to review the status of Y2K implementation within their command and the command of subordinate Component commands.
- The Senior Readiness Oversight Council was to report the readiness implications of Y2K.
- The Defense agencies were to report every Acquisition Category I, IA, and II system within their purview. The report was to address Y2K compliance or areas of noncompliance of each respective system.
- The Defense Information Systems Agency was to provide a report to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) by October 15, 1998, listing all Megacenter* domain users who failed to sign explicit agreements with the Defense Information Systems Agency by October 1, 1998. Based on the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) recommendations, the Office of the Under Secretary of Defense (Comptroller) was to withhold funds from the domain users named on the list.
- The Office of the Under Secretary of Defense (Comptroller) was to issue guidance to the Military Departments and Defense agencies on the funding prohibitions before October 1, 1998.

Additionally, the Secretary of Defense directed that the Military Departments, commanders in chief, and Defense agencies ensure that effective October 1, 1998:

- the list of mission-critical systems under their respective purview be accurately reported in the DoD Y2K database maintained by the Office of the Assistant Secretary of Defense (Command, Control,

*A Megacenter is a Defense Information Systems Agency organization that provides overall management, operations, and maintenance of all assigned information processing elements, ensuring responsive, reliable, and cost-effective processing services are provided to all customers.

Communications, and Intelligence), with each change in mission-critical designation reported and explained within 1 month of the change;

- funds are not obligated for any mission-critical system in the Y2K database that lacks a complete set of formal interface agreements for Y2K compliance;
- funds are not obligated for any information technology or national security system contract that processes date-related information and that does not contain the Y2K requirements specified in Federal Acquisition Regulation 39.106, "Year 2000 Compliance"; and
- funds are not obligated for any domain user in a Defense Information Systems Agency Megacenter if that domain user failed to sign all associated explicit test agreements with the Defense Information Systems Agency.

Y2K Verification. The Deputy Secretary of Defense issued the memorandum "Year 2000 (Y2K) Verification of National Security Capabilities" on August 24, 1998. The memorandum states that each of the directors of the Defense agencies must certify that they have tested the Y2K capabilities of their respective Component's information technology and national security systems in accordance with the DoD Management Plan. In addition, all Principal Staff Assistants of the Office of the Secretary of Defense were to verify that all functions under their purview will continue unaffected by Y2K issues. Each Principal Staff Assistant was required to provide the Deputy Secretary of Defense with plans for Y2K-related end-to-end testing of each process within communications, health/medical, intelligence, logistics, and personnel. Each Principal Staff Assistant was to certify that the test plan included:

- functional risk assessments,
- Y2K effects on continuity-of-business operations, and
- associated contingency plans.

Further, the test plans were to include all mission-critical systems involved in each test. The Director, Operational Test and Evaluation, was to help the Principal Staff Assistants with cross-functional, inter-Service, and cross-system testing.

Appendix D. Status of U.S. Army, Europe, and Seventh Army Year 2000 Program



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

January 19, 1999

MEMORANDUM FOR COMMANDER, U.S. ARMY, EUROPE, AND SEVENTH ARMY

SUBJECT: Assessment of U.S. Army, Europe, and Seventh Army Year 2000 Program Under the Follow-On Audit of the Year 2000 Issues Within U.S. European Command's Area of Responsibility (Project No. 8LG-5039.01)

This is an assessment of the U.S. Army, Europe, and Seventh Army year 2000 (Y2K) effort in support of the U.S. European Command, along with our suggested actions. The assessment is based on our visit from January 11 through 15, 1999, to the U.S. Army, Europe, and Seventh Army Headquarters, Heidelberg, Germany; 21st Theater Army Area Command, Kaiserslautern, Germany; 1st Personnel Command and 266th Finance Command, Schwetzingen, Germany; 5th Signal Command, Mannheim, Germany; and 104th Area Support Group, Hanau, Germany. Our review focused on functional participation, identification of critical systems, and operational contingency plans needed to perform core mission requirements.

The U.S. Army, Europe, and Seventh Army had established a Y2K program and had taken positive actions to address and resolve Y2K issues. As of January 15, 1999, the overall Y2K program at the U.S. Army, Europe, and Seventh Army and the subordinate commands we visited was in the renovation and implementation phases. The following areas need continued command emphasis.

Functional Participation. At the U.S. Army, Europe, and Seventh Army headquarters and the subordinate commands visited, the Y2K program was led by the Information Management staff; however, functional staffs were fully participating in the Y2K program. For example, the Deputy Commanding General, the Chief of Staff, and the functional staffs at U.S. Army, Europe, and Seventh Army headquarters and the subordinate commands periodically meet to review the status of contingency plans. DoD and Army standard systems, U.S. Army, Europe, and Seventh Army unique systems, weapon systems, facilities, host nation utilities, and network systems. In addition, functional staff at the 21st Theater Army Area Command was involved in determining mission-critical systems and developing work-arounds in the event of system failure. The continuation of full functional staff involvement in the U.S. Army, Europe, and Seventh Army Y2K program should ensure that the command will be prepared to address unanticipated disruptions because of Y2K problems.

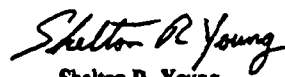
Mission-Critical Systems. At the organizations visited, functional staff identified mission-critical systems. In addition, the functional staff at the 21st Theater Army Area Command cross-checked the mission-critical systems to the mission-essential task list. Also, during our visit, U.S. Army, Europe, and Seventh Army headquarters was in the process of cross-checking its mission-critical systems to its mission-essential task list. The U.S. Army, Europe, and Seventh Army determined that its unique mission-critical systems are Y2K compliant and requested that the Army Audit Agency independently verify the Y2K compliance of those unique systems. Also, U.S. Army, Europe, and Seventh Army was proactively tracking the Y2K compliance status of DoD and Army standard systems by

searching the Internet, calling the program offices, and reviewing various DoD and Army databases. A central source of information on the Y2K compliance of DoD and Army standard systems was not yet readily available. Continuing to monitor the status of mission-critical systems should ensure that U.S. Army, Europe, and Seventh Army has sufficient information to assess potential Y2K impacts on its operational readiness.

Operational Contingency Plans. The U.S. Army, Europe, and Seventh Army was proactively developing operational contingency plans and expected to complete the plans in time to exercise them during the U.S. European Command operational evaluation scheduled for May 1999. The U.S. Army, Europe, and Seventh Army and its subordinate commands had received very little guidance from the Department of the Army on developing operational contingency plans; however, they proactively searched for operational contingency plans developed by other organizations and used them as a basis for developing their plans. For example, the 104th Area Support Group prepared a draft operational contingency plan for loss of electrical power, water, and environmental systems based on information obtained from the Internet, including the city of Cleveland's contingency plan. In addition, 21st Theater Army Area Command personnel stated that they routinely had system failures unrelated to the Y2K problem and were very familiar with using alternative procedures to perform their duties. Developing operational contingency plans in time for inclusion in the U.S. European Command operational evaluation should ensure that U.S. Army, Europe, and Seventh Army has workable procedures in place should it experience disruptions because of Y2K problems.

Overall, U.S. Army, Europe, and Seventh Army had made substantial progress in resolving its Y2K issues and in minimizing the potential adverse impact of Y2K on its mission to support the U.S. European Command. We commend U.S. Army, Europe, and Seventh Army and its subordinate commands for their efforts in involving all functional staffs in the Y2K program and in developing plans for future crises while simultaneously conducting an impressive schedule of operations. Accordingly, we consider the U.S. Army, Europe, and Seventh Army Y2K program in support of the U.S. European Command mission to be low risk.

Because of the time involved in completing the announced audit, we are providing you the results of our assessment in this form. We will issue a report upon completion of the audit that will include a copy of this letter and any comments you provide. Accordingly, we request that you provide any written comments you wish to make within 20 days of the date of this memorandum. Questions on the audit should be directed to Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172) (eklemstine@dodig.osd.mil) or Ms. Catherine M. Schneider at (703) 604-9609 (DSN 664-9609) (cschneider@dodig.osd.mil).


Shelton R. Young
Director, Readiness and
Logistics Support Directorate

cc:
Y2K Task Force, U.S. European Command
Chief Information Officer, Army
Auditor General, Department of the Army
Inspector General, Department of the Army
Joint Staff Y2K Office

Appendix E. Status of U.S. Naval Forces Europe Year 2000 Program



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

December 17, 1998

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. NAVAL FORCES EUROPE

SUBJECT: Assessment of U.S. Naval Forces Europe, Year 2000 Program Under the Follow-On Audit of Year 2000 Issues Within U.S. European Command's Area of Responsibility (Project No. 8LG-5039)

This is an assessment of the U.S. Naval Forces Europe Year 2000 (Y2K) effort in support of the U.S. European Command along with our suggested actions. The assessment is based on our October 1 through 16, 1998, visit to U.S. Naval Forces Europe, Fleet Air Mediterranean, and Naval Support Activity Naples, Italy. Our review focused on functional participation, identification of critical systems, and systems and operational contingency plans needed to perform core mission requirements.

The U.S. Naval Forces Europe had established a Y2K program and had taken positive actions to address and resolve Y2K issues. The U.S. Naval Forces Europe Y2K program started in July 1998 and was in the initial stage of implementation. The Command Y2K Project Office, Deputy Chief of Staff Command, Control, Communications, and Computers had developed a Y2K action plan and was aggressively pursuing its full implementation as were Y2K Project Offices at Fleet Air Mediterranean and Naval Support Activity Naples. However, the functional staffs of the three organizations did not fully participate in the program. The following problem areas need command attention.

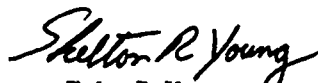
Functional Participation. At the organizations visited, the functional staff did not fully participate in the Y2K program. Without exception, the response was that Y2K was a systems problem and not my "functional" problem. Awareness is the first phase of the DoD five phased approach. The functional staff may have been aware of, but did not fully participate in the program. We suggest transitioning the Y2K lead from the Command, Control, Communications, and Computer Directorate to the Operations Directorate and adopting a "Tiger Team" approach that parallels the Headquarters U.S. European Command effort. This approach will ensure involvement of all functional staff in the Y2K program.

Mission Critical Systems. At the organizations visited, mission critical systems were identified by the technical staff Y2K Project Offices. Functional users of systems were not involved in the identification or prioritization of critical systems. In addition, the Y2K Project Offices and functional staffs were not aware of the Y2K status of all systems they were using. Accordingly, the commands did not have the information necessary to identify "show stopper" systems. We suggest the functional staff actively participate in the identification and prioritization of critical systems and designate an office to track and monitor the Y2K fixes of all critical systems. Identifying, prioritizing, and monitoring the status of mission critical systems will ensure the U.S. Naval Forces Europe has sufficient information to assess potential Y2K impacts on its operational readiness.

Operational Contingency Plans. At U.S. Naval Forces Europe and Fleet Air Mediterranean there were no operational contingency plans covering Y2K issues or any proactive efforts to develop them. The functional staff at those two commands were waiting for the systems program managers to provide system contingency plans addressing potential system failures and workarounds necessary to sustain mission critical capabilities. After system program managers provide system contingency plans, the functional staff at U.S. Naval Forces Europe and Fleet Air Mediterranean stated that they would prepare operational contingency plans. However, Naval Support Activity Naples was not waiting for system contingency plans, but was incorporating a Y2K scenario into its local disaster plan that was being tested. We recognize that system contingency plans are not due until December 31, 1998, and operational contingency plans are not due until March 31, 1999. However, U.S. Naval Forces Europe and Fleet Air Mediterranean should be proactive in obtaining the system contingency plans in order to have as much time as possible to prepare operational contingency plans before the April 1999 U.S. European Command operational evaluation.

Overall, U.S. Naval Forces Europe needs to improve its Y2K program to minimize the potential adverse effect of Y2K on its mission to support the U.S. European Command. Progress has been made by the Y2K Project Offices of U.S. Naval Forces Europe, Fleet Air Mediterranean, and Naval Support Activity Naples. However, the functional staffs have not fully accepted the program as an operational readiness issue. Accordingly, we consider the U.S. Naval Forces Europe Y2K program in support of the U.S. European Command mission to be high risk.

Because of a delay in completing the announced audit, we are providing you the results of our assessment in this form. We will issue a report upon completion of the audit that will include a copy of this letter and a summary of corrective actions taken by the command. Accordingly, we request that you inform us in writing within 30 days of the date of this memorandum of your planned actions. Questions on the audit should be directed to Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172) (eklemstine@dodig.osd.mil) or Ms. Catherine M. Schneider at (703) 604-9609 (DSN 664-9609) (cschneider@dodig.osd.mil).


Shelton R. Young
Director, Readiness and
Logistics Support Directorate

cc:
Y2K Task Force, U.S. European Command
Chief Information Officer, Department of Navy
Auditor General, Department of Navy
Naval Inspector General
Joint Staff Y2K Office



DEPARTMENT OF THE NAVY

COMMANDER IN CHIEF
UNITED STATES NAVAL FORCES, EUROPE
PSC 802
FPO AE 08498-0151

2000
N6Y2K/082
25 JAN 99

From: Commander in Chief, U.S. Naval Forces, Europe
To: Inspector General, Department of Defense
Subj: ASSESSMENT OF U.S. NAVAL FORCES EUROPE YEAR 2000 (Y2K)
PROGRAM (PROJECT NO. 8LG-5039)
Ref: (a) DODIG memo of 17 Dec 98

1. Reference (a) provides DOD IG assessment of the following areas of the CINCUSNAVEUR Year 2000 (Y2K) program: Functional Participation, Identification of Critical Systems, Operational Contingency Plans and Overall Status. Corrective actions and initiatives are provided below to address issues raised.

2. Functional Participation:

a. Issue. "At the organizations visited, the functional staff did not fully participate in the Y2K program. Without exception, the response was that Y2K was a systems problem and not my "functional problem."

b. Recommendation. Transition the Y2K lead from the Command, Control, Communications and Computers (C4) Directorate to the Operations Directorate and adopt a "Tiger Team" approach that parallels the Headquarters U.S. European Command effort.

c. Action Taken. CINCUSNAVEUR functional organizations now fully participate in the Y2K Program, and are committed to meeting the Year 2000 challenge. A clear distinction has been made throughout the command that Y2K is NOT a system problem exclusive to N6, but is a "functional" problem, which affects all aspects of the command. An Executive Steering Committee (ESC) comprised of the Chief of Staff, key Deputy Chiefs of Staff and Command Assistants, meets weekly to monitor the implementation of CINCUSNAVEUR's Y2K Action Plan. Dedicated Site Y2K points of contact have been assigned throughout the theater, with base-wide "Tiger Teams" established. To support USCINCEUR Y2K Task Force efforts, including the USCINCEUR Y2K OPEVAL scheduled 26 April to 6 May 1999, CINCUSNAVEUR appointed Y2K functional points of contact to liaison with their counterparts on the USCINCEUR Y2K Task Force.

3. Mission Critical Systems:

a. Issue. "Functional users of systems were not involved in the identification or prioritization of critical systems. In addition, the Y2K Project Offices and functional staffs were not aware of the Y2K status of all systems they were using.

Subj: ASSESSMENT OF U.S. NAVAL FORCES EUROPE YEAR 2000 (Y2K)
PROGRAM (PROJECT NO. 8LG-5039)

Accordingly, the commands did not have the information necessary to identify 'show stopper' systems."

b. Recommendation. Functional staff actively participate in the identification and prioritization of critical systems and designate an office to track and monitor the Y2K fixes of all critical systems.

c. Actions Taken

(1) In April 1998, CINCUSNAVEUR identified and categorized computer systems that could impact NAVEUR's support of USCINCEUR's warfighting mission if not Y2K compliant. Program of Record systems and some infrastructure in theater were categorized as high, medium, low or no impact. Those systems, along with any additional systems identified in the past quarter, are being tracked by the NAVEUR Y2K Project Office via the DOD Y2K Database, Navy Y2K Tracking System (NY2KTS) Database, and contact with Program Managers and System Commands.

(2) CINCUSNAVEUR prioritization strategy is to categorize non-compliant items, and determine which items are to be renovated or replaced. Items are to be grouped as either mission-critical or mission-support. Facilities embedded systems (FES) categorized as unknown, where vendors have not responded for 30 days, will be reported and treated as non-compliant. Theater prioritization of non-compliant items will be completed during a VTC scheduled 28 January 1999. Prioritization of FES based on mission-risk categories assigned will identify "show stopper" systems requiring renovation.

4. Operational Contingency Plans:

a. Issue. "At U.S. Naval Forces, Europe and Fleet Air Mediterranean there were no operational contingency plans covering Y2K issues or any proactive efforts to develop them."

b. Recommendation. U.S. Naval Forces, Europe and Fleet Air Mediterranean be proactive in obtaining Contingency Plans in order to have as much time as possible to prepare Continuity of Operations Plans before the April 1999 U.S. European Command operational evaluation.

c. Action Taken. Formal guidance on Contingency Planning (CP) and Continuity of Operations Planning (COOP) provided by CINCUSNAVEUR, along with Navy-wide guidance provided in the Navy CP and COOP Guide, increased sites understanding the difference between CPs written for systems, and COOPs written for mission-critical functions. To date, a total of 85 of 88 required COOPs are in place for mission-critical functions including facilities, maintenance, and C4 systems. The remaining three COOPs will be

Subj: ASSESSMENT OF U.S. NAVAL FORCES EUROPE YEAR 2000 (Y2K)
PROGRAM (PROJECT NO. 8LG-5039)

completed by 31 January 1999. Of the 88 COOPs, 31 of 33
facilities-related COOPs are in place.

5. CINCUSNAVEUR Overall Progress:

a. Issue. "Overall, progress has been made by the Y2K Project Offices of U.S. Naval Forces, Europe, Fleet Air Mediterranean, and Naval Support Activity Naples. However, the functional staffs have not fully accepted the program as an operational readiness issue. Accordingly, we consider the U.S. Naval Forces, Europe Y2K program in support of the U.S. European Command mission to be high risk."

b. Recommendation. U.S. Naval Forces, Europe improve its Y2K program to minimize the potential adverse effect of Y2K on its mission to support the U.S. European Command.

c. Plan of Action and Milestones (POA&M):

(1) CINCUSNAVEUR has completed the following milestones the past five months:

- (a) Promulgation of CINCUSNAVEUR Y2K Action Plan.
- (b) Completed all Facilities Embedded Systems (FES) assessments.
- (c) Commencement of IT renovation throughout AOR.
- (d) Completed 86 of 104 CPs and COOPs.

These accomplishments have helped CINCUSNAVEUR make up some lost time, now meeting implementation deadlines only five months, vice 12 months, behind schedule.

(2) Remaining milestones to be met are:

(a) Renovation:

(1) Receipt of IT upgrades at sites by March 1999.

(2) Renovation of FES based on Theater Prioritization List for Y2K fixes, 1 April 1999.

(b) Validation:

(1) Promulgation of the CINCUSNAVEUR Testing and Certification Plan, 31 January 1999.

(2) Distribution and installation of the CLICKNET Y2K IT Testing Tool throughout the AOR, 31 Jan 1999.

Subj: ASSESSMENT OF U.S. NAVAL FORCES EUROPE YEAR 2000 (Y2K)
PROGRAM (PROJECT NO. 8LG-5039)

(c) Implementation:

(1) Integration of Programs of Record Y2K
upgrades into existing infrastructure.

(2) Implementation/installation of FES Y2K fixes.

(3) Following management oversight will continue:

(a) Tracking of remaining phases for theater Program
of Record systems.

(b) Planning and participation in EUROM Y2K OPEVAL.

(c) Participation, as required, in Y2K conferences,
exercises, etc.

(d) Supporting COOP revision and testing process.

(e) Weekly ESC and monthly DCINC briefs.

(f) Y2K briefs for various visits and conferences.

(g) Periodic updates to the NY2KTS database.

R. S. Dearth

R. S. DEARTH
Chief of Staff

Appendix F. Status of U.S. Air Forces in Europe Year 2000 Program



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

January 12, 1999

MEMORANDUM FOR COMMANDER, U.S. AIR FORCES IN EUROPE

SUBJECT: Assessment of U.S. Air Forces in Europe Year 2000 Program Under the Follow-On Audit of the Year 2000 Issues Within U.S. European Command's Area of Responsibility (Project No. 8LG-5039.01)

This is an assessment of the U.S. Air Forces in Europe year 2000 (Y2K) effort in support of the U.S. European Command, along with our suggested actions. The assessment is based on our October 5 through 9, 1998, visit to the U.S. Air Forces in Europe Headquarters, Ramstein, Germany, and our November 30 through December 16, 1998, visit to the 48th Air Wing, Royal Air Force Lakenheath, United Kingdom; the 31st Air Wing, Aviano Air Base, Italy; and the 52nd Air Wing, Spangdahlem Air Base, Germany. Our review focused on functional participation, identification of critical systems, and operational contingency plans needed to perform core mission requirements.

The U.S. Air Forces in Europe had established a Y2K program and had taken positive actions to address and resolve Y2K issues. As of December 16, 1998, the status of the Y2K program at the U.S. Air Forces in Europe and the subordinate commands we visited ranged from the end of the assessment phase at Aviano Air Base to the beginning of the implementation phase (fix, repair, or ignore noncompliant systems/equipment) at Royal Air Force Lakenheath. The following concerns needed command attention

Functional Participation. At the U.S. Air Forces in Europe Headquarters and the air wings visited, functional staffs fully participated in the Y2K program. Each functional area of the wings participated by assigning Y2K representatives at the squadron level. However, Y2K continuity of operations plans were not being developed as overall wing plans. Until our visit to each air base, the communications squadron of each wing was developing the continuity of operations plan without overall wing coordination. To develop an overall wing plan requires the coordination of the wing planning squadrons to ensure that existing contingency plans are considered and that wing resources can be used where most needed should Y2K system failures occur. We suggest that wing Y2K continuity of operations plans include existing contingency plans coordinated to ensure optimal use of resources. That approach will ensure a coordinated involvement of all functional staff in the Y2K program.

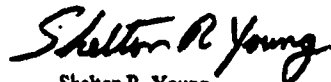
Mission Critical Systems. At the wings visited, squadron representatives identified mission critical systems; and wing Y2K representatives gathered and reassessed squadron lists of mission critical systems to ensure uniform prioritization. The exception was the aircraft and weapons systems such as the F-15 fighter aircraft and associated systems. A reliable source of information on the Y2K compliance of aircraft and weapons systems was not readily available to wing personnel. We suggest that U.S. Air Forces in Europe Y2K

personnel ensure that wing commanders are made aware of the Y2K status of all war-fighting assets under their authority. Identifying, prioritizing, and monitoring the status of mission critical systems will ensure that U.S. Air Forces in Europe have sufficient information to assess potential Y2K impacts on its operational readiness.

Operational Contingency Plans. The U.S. Air Forces in Europe is proactively developing continuity of operations plans and expects to complete them by January 31, 1999. The proactive approach of wing commanders will result in contingency plans being developed in time for use during the April 1999 U.S. European Command operational evaluation. The three wings we visited were preparing Y2K continuity of operations plans in accordance with Air Force Instruction 10-232, "Year 2000 Continuity of Operations," September 3, 1998. Although behind the initial completion date of December 31, 1998, the plans should be completed by January 31, 1999. We suggest that U.S. Air Forces in Europe commend wing commanders for their efforts in developing plans for future crises while simultaneously conducting an impressive schedule of air operations.

Overall, U.S. Air Forces in Europe needs to improve its Y2K program to minimize the potential adverse effect of Y2K on its mission to support the U.S. European Command. The Y2K organizations along with the 48th, 31st, and 52nd Air Wings have made much progress. However, the wings must ensure that existing contingency plans of all functional elements are considered in the overall wing continuity of operations plan and the Y2K status of wing war-fighting assets is made available to wing personnel. Accordingly, we consider the U.S. Air Forces in Europe Y2K program in support of the U.S. European Command mission to be moderate risk.

Because of a delay in completing the announced audit, we are providing you the results of assessment in this form. We will issue a report upon completion of the audit that will include a copy of this letter and a summary of corrective actions taken by the command. Accordingly, we request that you inform us in writing within 30 days of the date of this memorandum of your planned actions. Questions on the audit should be directed to Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172) (eklemstine@dodig.osd.mil) or Mr. Timothy E. Moore at (703) 604-9639 (DSN 664-9639) (tmoore@dodig.osd.mil).



Shelton R. Young
Director, Readiness and
Logistics Support Directorate

cc:
Y2K Task Force, U.S. European Command
Chief Information Officer, Air Force
Auditor General, Department of the Air Force
Inspector General, Department of the Air Force
Joint Staff Y2K Office



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCES IN EUROPE

25 FEB 1999

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

FROM: USAFE/SC

SUBJECT: Assessment of U.S. Air Forces in Europe Year 2000 Program under the Follow-On Audit of the Year 2000 Issues within U.S. European Command's Area of Responsibility (Project No. 8LG-5039.01) (Your memo, same subject, 12 Jan 99)

1. The following reply is submitted in response to the referenced memo. The areas inspected are listed below with USAFE's corrective actions and status.

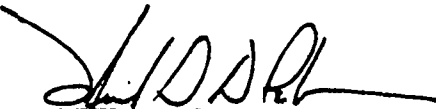
Continuity of Operations Planning: Per Air Force Instruction 10-232, Continuity of Operations Planning (COOP), USAFE wings are actively pursuing completion of the planning cycle. Expect all wings plans to be complete by 15 Mar 99 and a comprehensive USAFE plan to be presented by 15 Apr 99.

Mission Critical Systems: In the past we relied upon the Air Force Automated Systems Inventory (AFASI) database to provide wing and group commanders with Y2K information on major weapons systems. Following your visit, we contacted wing Y2K offices to ensure they had ready access to AFASI. We also supplemented that information with updates to commanders and staff by the Air Force Materiel Command Y2K program office.

Operational Contingency Plans: USAFE formed a Year 2000 "Tiger Team" composed of experts from its directorates that have mission-critical Y2K vulnerabilities. Our team will conduct Staff Assistance Visits (SAVs) to all six of USAFE's Main Operating Bases (MOBs). Visits will be conducted in March and April.

2. Given the actions outlined above and our overall Y2K program efforts, USAFE's Y2K status in support of EUCOM should be categorized as low risk.

3. My POC on this matter is Col Wayne Scott, DSN 480-7230, email: css.cc@ramstein.af.mil.


MICHAEL W. PETERSON
Colonel, USAF
Director, Communications and Information

Appendix G. Status of the North Atlantic Treaty Organization Year 2000 Program

As of October 1998, NATO had developed a Y2K program and had drafted a Y2K plan. NATO had established a Y2K working group that was completing the awareness phase and beginning the assessment phase. Though NATO had assumed a Y2K management role, NATO Agencies and Commands maintained responsibility for Y2K fixes.

During September 1998, the NATO Y2K working group hired three contractors and established the NATO Y2K Support Cell. The Support Cell constructed and populated a NATO Y2K database that included mission-critical and non-mission-critical systems. As of January 29, 1999, the NATO database included 307 systems, 125 of which were mission-critical. The following table shows the Y2K status of the mission-critical systems.

NATO Mission-Critical Systems	
<u>Status</u>	<u>Number of Systems</u>
Compliant	10
Not compliant	29
Under investigation	4
Unknown	<u>82</u>
Total	125

Upon completing the database, the Support Cell planned to prioritize systems according to mission criticality. NATO had established a requirement that all mission-critical and non-mission-critical systems would have contingency plans but had not identified all system interfaces, and interface agreements were not in place.

Appendix H. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications,
Intelligence, Surveillance, Reconnaissance, and Space Systems)
Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief
Information Officer Policy and Implementation)
Principal Director for Year 2000
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Chief Information Officer, Army
Commander, U.S. Army, Europe, and Seventh Army
Inspector General, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Navy
Commander in Chief, U.S. Naval Forces Europe
Inspector General, Department of the Navy
Auditor General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Air Force
Commander, U.S. Air Forces in Europe
Inspector General, Department of Air Force
Auditor General, Department of the Air Force

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
 Inspector General, Defense Information Systems Agency
 Chief Information Officer, Defense Information Systems Agency
 United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
 Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
 Office of Information and Regulatory Affairs
General Accounting Office
 National Security and International Affairs Division
 Technical Information Center
 Accounting and Information Management Division
 Director, Defense Information and Financial Management Systems

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Committee on Government Reform

House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform

House Subcommittee on National Security, Veterans Affairs, and International Relations,
Committee on Government Reform

House Subcommittee on Technology, Committee on Science

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

Final Report
Reference



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

2 APR 1999

MEMORANDUM FOR DIRECTOR, READINESS AND LOGISTICS SUPPORT
DIRECTORATE, INSPECTOR GENERAL, DOD

SUBJECT: Audit Report on Year 2000 Issues Within U.S. European Command and Its Service
Components (Project No. 8LG-5039.01)

This office has reviewed the Draft Audit Report on the Year 2000 Issues Within U.S. European
Command and Its Service Components, dated February 12, 1999

We recommend that the report be modified to include the following general statements: Page 12,
paragraph 2: Access to DoD Y2K Database. Information on how users at the unified commands will
obtain training on the new Carnegie Mellon database has been distributed to the Joint Staff for further
dissemination to the unified commands. A request has been submitted to the Joint Staff for Y2K POCs
for the unified commands so in the future, OSD can deal directly with the unified commands.

Page 13

Page 12, paragraph 3: Carnegie Mellon Y2K Database. Copies of the Carnegie Mellon users
manual have been given to the Joint Staff. The Joint Staff as the administrator for the unified commands,
has the responsibility to filter all guidance from OSD down to the unified commands. As stated earlier, a
request has been submitted to the Joint Staff for Y2K POCs for the unified commands so in the future,
OSD can deal directly with the unified commands.

Page 13


Page 13, paragraph 4: Status of Access to Y2K Systems Information. The database is accessible
via the World Wide Web with a 128 Bit Domestic Browser. The DISA URL for a free copy of a 128 bit
domestic browser was provided to all administrators. If the unified commands don't have the required
browser on their PCs, they will have to download the required version. Any additional access problems
to the site are being worked on a case by cases basis once OSD is notified that there is a problem.

Page 14

Page 14, paragraph 2: Configuration Management. The Office of the Secretary of Defense Y2K
Program Office is currently working on a configuration management policy for DoD Y2K systems to
ensure that all DoD software development and software maintenance programs have established
procedures. It was expected that a baselined version of the software incorporating all Y2K fixes be
established upon completion of the five-phase program. The Y2K-compliant version of the system
should be used for OPEVAL or functional end-to-end testing.

Page 15

My point of contact for any additional information is Mr. Willie Moss at (703)
602-0980 ext 105.


William A. Curtis
Principal Director, Year 2000



U.S. European Command Comments



HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
Office of the Chief of Staff
APO AE 09128

01 APR 1999

ECCS

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE

SUBJECT: Response to Audit Draft Report of Year 2000 (Y2K) Issues Within U.S.
European Command and Its Service Components (Proj # 8LG-5039.01)

1. EUCOM welcomes your assistance as we lean forward to meet the Year 2000 (Y2K) challenge. Our comments on your draft February 1999 assessment of the U.S. European Command's Year 2000 program are attached.
2. We concur with your recommendations, although much has happened since your investigation was completed. In conjunction with the Joint Staff, we are continually improving our Y2K guidance and program implementation. In some cases, USEUCOM must rely on the Joint Staff, Components, Services, and external agencies to provide information concerning Y2K compliance. Communication channels with these various elements remain constantly open, but provide unique challenges to monitoring Y2K compliance.
3. Your audit efforts are an important contribution to our overall management improvement programs. We look forward to working with your audit teams in the future.

A handwritten signature in dark ink, appearing to read "M. A. Canavan", is positioned above the typed name and title.

MICHAEL A. CANAVAN
Lieutenant General, USA
Chief of Staff

COMMENTS ON DRAFT REPORT OF AUDIT
"U.S. EUROPEAN COMMAND YEAR 2000 ISSUES"

Summary of Recommendations Section

1. Recommendation: Ensure users of the Carnegie Mellon database have the appropriate equipment that allows them to access the database.

USEUCOM Response: Concur. Carnegie-Mellon database file is currently being distributed via email to all Component commands and the USEUCOM Y2K taskforce will continue to distribute it via email until it comes on-line.

2. Recommendation: Complete systems architectures to determine Y2K status for all mission-critical functional areas.

USEUCOM Response: Concur with comment. Components report monthly on ten functional areas with respect to Y2K compliance. Current focus of detailed system architectures is in support of the June 1999 NEO/Peacekeeping and Non-Strategic Nuclear Forces Operational Evaluations (OPEVALs). Under the CJCS OPEVAL program, each CINC is assigned a specific mission area to ensure that between all the CINCs, all mission critical functions are analyzed. USEUCOM has completed detailed systems architectures for the mission critical strategic tasks, and the subordinate operational and tactical tasks related to NEO/PKO, per JCS guidance. Upon completion of our NEO/PKO OPEVALs, this command will continue to monitor and report on the Y2K status of the mission-critical functions from the below ten functional areas that are not addressed in any of the CJCS OPEVALs:

- A. NUCLEAR COMMAND AND CONTROL (C2)/SPECIAL WEAPONS SYSTEMS
- B. WEAPONS SYSTEMS (TANKS/PLANES/SHIPS)
- C. C2 SYSTEMS (NON-NUCLEAR)
- D. COMMUNICATIONS SYSTEMS
- E. INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYSTEMS
- F. INFRASTRUCTURE (FACILITIES/INDUSTRIAL/PRODUCTION) SYSTEMS
- G. MOBILITY SYSTEMS
- H. SUSTAINMENT SYSTEMS
- I. PERSONNEL SYSTEMS
- J. OTHER AREAS AS REQUIRED

3. Recommendation: Assess the risk of establishing a moratorium on system changes the last 3 months of calendar year 1999.

USEUCOM Response: Concur. This command supports the Joint Staff recommendation that the CINC have the ultimate authority to grant a waiver to any such moratorium (regardless of the time) allowing the flexibility to make or deny changes based on a case by case risk assessment. USEUCOM will publish configuration

management guidance for all systems in theater after DOD/JCS publishes higher headquarters guidance, which is currently in development and staffing.

4. Recommendation: Include a representative from the Command Surgeon's office (ECMD) on the USEUCOM Task Force, coordinate with the Military Department medical commands, the Office of the Assistant Secretary of Defense (Health affairs), and USTRANSCOM to obtain Y2K status of Health care systems used in EUCOM theater.

USEUCOM Response: Partially Concur with recommendations. ECMD has provided LCDR Bob Welch as the medical representative. Due to manpower shortages, ECMD was unable to provide a full-time representative to the Y2K TF, but LCDR Welch has been very involved in the Y2K effort and the task force's activities. Medical issues are not taken lightly and the EUCOM Surgeon's Office (ECMD) is working diligently. The Medical Representative from ECMD is assigned to this Command as the Medical Chief Information Officer (CIO) for USEUCOM. His primary duties are related to medical information systems. Y2K is one of his priorities. Since the IG visit, the USEUCOM Task Force Medical representative met with Information Systems Officers / Chief Information Officers for the Components in theater and requested their support in providing information as it relates to medical Y2K in theater. The Medical Representative also had discussions with Joint Staff (J-4, Medical Readiness Division) on how to stay current on Y2K as it relates to TRANSCOM and Health Affairs. Both sides agreed that J-4, MRD will continue to provide information to EUCOM (when available) as it relates to OASD(HA) and TRANSCOM Y2K issues. We concur with your recommendation to coordinate but recommend IG stress to Service Components, OASD(HA), and TRANSCOM to provide EUCOM with courtesy copies on all related Y2K issues. The USEUCOM Task Force actively seeks information from the Services and Health Affairs. However, the Unified Commands are not in the reporting chain for Y2K issues involving Medical systems. Your assistance in ensuring Service Components, OASD(HA), and TRANSCOM info all CINCs on medical issues will ensure we have the most current information.

Action: USEUCOM will undertake to include another functional category in its monthly report on Y2K status: Medical. This will give the CINC and his representatives more direct oversight of the medical Y2K efforts in theater.

5. Recommendation: Prepare all required operational contingency plans by March 31, 1999.

USEUCOM Response: Partially Concur. USEUCOM and its components are focusing on both operational Contingency Plans (CPs) (plans for action taken regarding a system due to a Y2K failure), and Continuity Of Operations Plans (COOPs) (plans to work around a Y2K failure to ensure the critical task is accomplished) which are required for the JCS-directed OPEVAL. After completion of this event, additional focus will be placed upon Intelligence, Reconnaissance, and Surveillance CPs and COOPs to ensure readiness for the JCS J7 run Chairman's Contingency Assessment POSITIVE

RESPONSE Y2K-3, which the theater will undergo in June. Third priority is to finalize CPs and COOPs for other systems not addressed in the OPEVAL and the CCA. Anticipate this will be accomplished NLT 30 SEP 99. USEUCOM plans a series of contingency tabletop exercises to validate the critical CPs and COOPs and ensure the entire theater is ready for potential Y2K outages.

6. Recommendation: Include Aircraft and Weapon systems in the OPEVAL.

USEUCOM Response: Partially Concur. USEUCOM will include aircraft and weapons systems in the OPEVAL effort, but not in the physical event, 12-22 May 1999. The focus of this event is mission critical joint systems, interfaces between them and service systems, and cross service systems and interfaces. Methodology we are using for OPEVAL strictly follows Joint Staff guidance -- and they concur with not including actual shooters in the OPEVAL. This is because service Y2K efforts do not address these areas and these are the areas where the highest risk of a system of systems' Y2K failure exists. Services will be conducting robust evaluations of their service unique systems, including weapons platforms, per title 10. USEUCOM plans on conducting a complete review of these efforts to ensure that the defined thin lines and critical tasks, which are part of EUCCOM's definition, are evaluated in the service (or other CINC) efforts. This will ensure a 100% evaluation, from "CINC's HQs down to the beach," of the theater's entire mission critical thin line of systems. A "virtual end-to-end" OPEVAL will then be completed by coupling the EUCCOM executed OPEVAL with the multiple service efforts. This will save resources, avoid redundancy, spread the efforts among many participants, and keep the responsibility for systems evaluation with the primary owner and users of the system of systems (be it joint or service unique).

7. Recommendation: Invite NATO to participate in the peacekeeping portion of the OPEVAL.

USEUCOM Response: Partially Concur. The USEUCOM OPEVAL only involves U.S. systems. We, as do all other CINCs, recognize the importance of NATO in support of U.S. interests. However, USEUCOM cannot ensure allied/coalition systems are operationally evaluated. Recommend this initiative come from the Joint Staff and/or OSD. USEUCOM stands ready to provide advice, assistance, participation, or oversight JCS tasks this command to provide. This command continues to do what is possible until that occurs. Efforts include:

- Identification of all possible interfaces and reporting these to Joint Staff
- Identification of all current/planned U.S. system interfaces with allied nations
- Dialog with Supreme Headquarters Allied Powers Europe (SHAPE)
- Recommending that the Joint Staff initiate a NATO effort through the national military representative.

8. Recommendation: Issue guidance for uniformly addressing host nation infrastructure issues in theater, establish a central office within the European theater for maintaining Y2K compliance data on host nation infrastructure.

USEUCOM Response: Concur. The USEUCOM Y2K Task Force is the central office for European Theater host nation issues. Our ECJ4 representative is on-board with component issues, scheduled for formal training (April 1999) and has a draft plan to be published in AUG 1999 to formally provide direction and oversight for EUCOM theater host nation issues. The components, at the direction of their services, have robust programs for host nation interaction, infrastructure validation, and back-up contingencies. USEUCOM monitors component preparedness in this area through the monthly report, where infrastructure is one of the nine functional categories.

9. Recommendation: Identify and validate funding requirements.

USEUCOM Response: Concur. USEUCOM received Joint Staff funds to support the known in-Theater Year 2000 efforts.

10. USAREUR, USAFE, NAVEUR and MARFOREUR Command responses

Component responses follow.

*

*USAREUR comments follow. NAVEUR comments are in Appendix E; USAFE comments are in Appendix F; and MARFOREUR comments are not included because they were in email format and concurred with the report.



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
THE DEPUTY CHIEF OF STAFF, INFORMATION MANAGEMENT
UNIT 28351
APO AE 09014

AEAIM-IS (25)

18 March 1999

MEMORANDUM FOR U.S. European Command, ATTN: ECJ3-Y2K, UNIT 30400, BOX
1000, APO AE 09128-4209

SUBJECT: Reply to DODIG Draft Report on Year 2000 Issues Within U.S. European
Command and Its Service Components (Project No. 8LG-5039.01)

1. The Deputy Chief of Staff, Information Management, U.S. Army, Europe and Seventh Army (DCSIM, USAREUR) has reviewed the subject draft report and concurs with the reasonableness of the facts and conclusions of each of the sections of the report that specifically deal with USAREUR. In addition, we appreciated the valuable assistance the DODIG team members provided during their visit in January 1999. DODIG's assessment was extremely helpful in determining the adequacy of our Year 2000 (Y2K) Program. Further, the results of the visit will assist in preparing for the challenges and prioritizing future actions to prevent Y2K system failures. We would like to offer the following comments in response to the subject draft report.

a. Page 5 of the draft report. The USAREUR ODCSIM Y2K office currently has 11 staff members. The following is a summary of USAREUR's Y2K target completion dates (according to USAREUR reporting categories):

- 1) Office Automation: Done
- 2) Network Systems: 30 Apr 99
- 3) DA/DOD Standard Systems: 30 Sep 99
- 4) USAREUR Unique Systems: 30 May 99
- 5) Weapons Systems: 31 Jul 99
- 6) Non-Information Technology: 30 May 99

b. Page 11 of the draft report. All of USAREUR's Unique Systems are classified as major systems. Further, USAREUR is not responsible for renovating any mission-critical Information Technology (IT) systems. In addition, of the 16 remaining USAREUR Unique Systems that require renovation, 12 of the systems have interfaces with non-compliant DA or DOD Standard Systems. Consequently, USAREUR's functional proponents continue to expend great amounts of time researching the compliance status and renovation dates of IT systems.

Final Report
Reference

AEAIM-IS (25)

SUBJECT: Reply to DODIG Draft Report on Year 2000 Issues Within U.S. European Command and Its Service Components (Project No. 8LG-5039.01)

Page 21

c. Page 20 of the draft report. USAREUR staff agencies and commands are continuing to develop their operational contingency plans and expect complete initial drafts of all operational contingency plans by 31 Mar 99. Organizations will continue to refine and test their contingency plans throughout the year, particularly during the Operational Evaluations and installation testing.

Page 24-25

d. Page 23 of the draft report. Even though USAREUR did not meet the goal of awarding the centralized renovation contract by 15 Feb 99, USAREUR Area Support Groups will still have all facilities infrastructure items that would be adversely affected by the Y2K problem either repaired, or replaced, by 30 Jun 99. In fact, USAREUR is anticipating completing work in this area by 30 May 99.

Page 26

e. Page 25 of the draft report. USAREUR is still in the process of validating its list of Y2K requirements and finalizing its requirements prior to its mid-year fiscal review in mid-April 99.

2. If you have any questions, or require additional information, please contact MAJ Scott Barrington at DSN 370-8025 or by email at barringtonj@hq.hqusareur.army.mil.



L.A. Klooster
Colonel, G.S.
Assistant Deputy Chief of Staff,
Information Management

Department of the Army Comments



Office, Director of Information
Systems for Command, Control,
Communications, & Computers

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

10 MAR 1999

SAIS-IIAC

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, 400
ARMY NAVY DRIVE, ARLINGTON, VA 22202

SUBJECT: Draft Audit Report on Year 2000 Issues Within U.S. European Command
and Its Service Components (Project No. 8LG-5039.01)

Reference memorandum, February 12, 1999, subject: Audit Report on Year 2000
Issues Within U.S. European Command and Its Service Components (Project No. 8LG-
5039.01). As requested, the following Army response to subject draft report is provided:

**Recommendation 3: We recommend that the Army Year 2000 Program
Office issue operational contingency planning guidance.**

Response: Concur. The Army Year 2000 Program Office is in the process of
updating the Contingency Planning section of the Army Y2K Homepage to include more
guidance on operational contingency planning. In addition, the Army CIO is issuing a
Y2K policy update to all Army activities that includes guidance on both system and
operational contingency planning. Both efforts will be completed in March 1999.

My point of contact for this action is Mr. William Dates, 275-9483.

Miriam F. Browning
Director for Information
Management

CF: SAAG-PMO-L

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Shelton R. Young
Evelyn R. Klemstine
Catherine M. Schneiter
Andrew L. Forte
Walter Jackson
Timothy E. Moore
Robert T. Briggs
G. Paul Johnson
Bryon J. Farber
Cheryl L. Snyder
Mary A. Hoover

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Issues Within U.S. European Command and its Service Components

B. DATE Report Downloaded From the Internet: 08/23/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 08/23/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.